公安院校
招录培养体制改革
试点专业
系列教材

计算机犯罪侦查方向

丛书主编 李锦

# 互联网体系结构

曾刚 主编

清华大学出版社

公安院校招录培养体制改革试点专业系列教材

# 互联网体系结构

曾　刚　主编

清华大学出版社
北　京

## 内 容 简 介

本书系统地介绍了计算机网络体系结构，以及各层的原理与技术。主要内容包括计算机网络概述、网络体系结构及协议、物理层相关基础知识、数据链路层与局域网技术、网络层的主流协议、网络互联技术、传输层的主流协议、网络操作系统、Windows Server 2008 下应用层的主要应用技术。

本书结构清晰，内容丰富，紧贴实际，设计了大量的课后实验。本书适合于计算机及相关专业大学本科、专升本、高职高专等不同层次学生作为教材使用，也可以作为相关专业技术人员参考资料使用。



**图书在版编目(CIP)数据**

互联网体系结构/曾刚主编. --北京：清华大学出版社，2012.8
（公安院校招录培养体制改革试点专业系列教材）
ISBN 978-7-302-29183-1

Ⅰ. ①互… Ⅱ. ①曾… Ⅲ. ①互联网络－高等学校－教材 Ⅳ. ①TP393.4

中国版本图书馆 CIP 数据核字(2012)第 142871 号

**责任编辑：** 闫红梅 薛 阳
**封面设计：**
**责任校对：** 焦丽丽
**责任印制：**

**出版发行：** 清华大学出版社
**网　　址：** http://www.tup.com.cn，http://www.wqbook.com
**地　　址：** 北京清华大学学研大厦 A 座　　**邮　　编：** 100084
**社 总 机：** 010-62770175　　**邮　　购：** 010-62786544
**投稿与读者服务：** 010-62776969，c-service@tup.tsinghua.edu.cn
**质量反馈：** 010-62772015，zhiliang@tup.tsinghua.edu.cn
**课件下载：** http://www.tup.com.cn，010-62795954
**印 刷 者：**
**装 订 者：**
**经　　销：** 全国新华书店
**开　　本：** 185mm×230mm　　**印　　张：** 19.25　　**字　　数：** 419 千字
**版　　次：** 2012 年 8 月第 1 版　　**印　　次：** 2012 年 8 月第 1 次印刷
**印　　数：** 1～　000
**定　　价：** 　.00 元

产品编号：044602-01




期待已久的由李锦同志主编的《公安院校招录培养体制改革试点专业系列教材》终于出版了！该系列教材是我国第一套计算机犯罪侦查专业系列教材，它的出版解决了国内相关院校教师与学生急需的教课书问题，也为从事信息安全专业和侦查执法人员提供一套极有价值的参考丛书。这实属一件可喜可贺的事！

由于信息技术空前迅速的发展，极具挑战的计算机网络空间形成了一个变幻无穷的虚拟空间。现实社会中的犯罪越来越多地涉及到计算机、手机等工具，各种数字技术与网络虚拟空间的交汇，使计算机犯罪侦查技术变得空前重要与紧迫。从 20 世纪 90 年代兴起的数字取证调查，涌现出各种各样的技术和工具，使得数字取证成为计算机专业的一门新兴学科。国际上的一些大学近年来已设置了专门的系和研究生学位的授予，为计算机犯罪侦查的教学内容增添了丰富而又精彩的情景。他山之石可以攻玉，许多技术和教材可以借鉴，但数字取证牵涉到法学、法规，各国的国情不尽相同，唯一的解决办法就是必须自主创新、撰写适合国内需要的相应教材。

面临这一劈山开路的挑战，本教材从专业的技术层面为国内的本科生尝试提供全面的教学培训，内容包括了从互联网体系结构原理到电子商务应用与各种法规，以及计算机网络攻防技术与信息系统安全等级保护与管理等基础知识，重点围绕着计算机犯罪调查的手段、工具与方法以及数据证据的分析与鉴定等基础知识；教材注重在传授理论知识的同时，强化面向实战能力的培训，全套教材既适应了学科特点又考虑到学生层次的具体情况，处处反映出作者们的精心思索。

本系列教材参编的作者全部来自辽宁警官高等专科学校的师资队伍，该校地处辽东半岛，面临蓝色的大海，大浪淘沙涌现一批时代的人杰。庄严整洁的校园具有公安教育突出的特色，更为可贵的是他们倡导教学、科研、警务实践紧密结合，不断创新教学模式的一贯校风，每年从那里培养出大量信息时代专业特色明显、创新能力强的人才队伍。本套系列教材的出版充分体现了该校的学术水平与精神面貌，尤其映射出参编作者们拥有第一线资深的教学经验和扎实的实际专业知识，以及始终保持一股奋发上进、开拓创新的风范。我在此由衷地对本教材的出版表示祝贺，并预祝他们再接再厉，取得更加辉煌的成功！

许榕生

2012-6 写于北京




# 前言

互联网体系结构是计算机专业、网络安全专业等相关专业的核心课程之一，编者在编写这本教材的时候，参考了大量国内外相关书籍及较新资料，希望本书能够适应新形势下网络安全专业的教学需要。

本书的特色：

(1) 本书以互联网体系结构为主线，根据网络体系结构在各层介绍了协议、功能、相关技术。

(2) 突出实际应用，本书以实际应用为导引，多数章节在讲解理论基础知识的同时，以实验为载体，突出了对学生动手能力和创新能力的培养。

(3) 本书各章均配有大量的思考与练习题，帮助学生加深对各章节内容的理解。

全书共分为13章。

第1章介绍了计算机网络概述。包括网络的定义，网络的产生和发展，网络的主要功能，网络的拓扑结构，网络的分类，网络的组成等。

第2章介绍了计算机网络体系结构。包括网络体系结构概述，ISO与OSI参考模型，TCP/IP参考模型以及两种体系结构的比较。

第3章介绍了物理层相关的数据通信基础知识。包括基本概念，数据传输方式，传输介质，数据交换技术等。

第4章介绍了数据链路层与局域网相关技术。包括局域网概述，虚拟局域网，无线局域网和局域网组网实例等，这一章还设计了4个相关实验。

第5章介绍了网络层的主流协议。包括IPv4和IPv6，ARP和RARP协议，ICMP协议等。

第6章介绍了网络互联技术。主要介绍了网络互联设备，路由器和路由选择，路由器的配置等，本章配合理论知识，设计了9个网络实验。

第7章介绍了传输层的主流协议。包括传输层协议概述，TCP协议，UDP协议等。

第8章介绍了网络操作系统。介绍了操作系统相关的概念，简单地介绍了UNIX，Linux，NetWare，Windows几种操作系统，最后讲述了Windows 2008的特点及基本设置。

由于篇幅的原因应用层的主要应用技术分布到第9～13章。除了介绍每种应用的原理、基本配置方法外，还重点突出了安全方面的考虑，每章后面也附了相关实验。

本书第1、8、9、10、11、12、13章由曾刚编写，第2章由常艳编写，第3、7章由大连职业技术学院杨文艳编写，第4章由刘洋洋编写，第5章由闫威编写，第6章由孙永义、陈旭编写，最后由曾刚统稿。本书在编写过程中得到了众多专家学者的支持与帮助，这里表示衷心的感谢。

招录体制改革后，招收的网络安全专业体改生多来自不同院校的计算机相关专业，他们的知识体系不同，动手实践能力不同，因此，在教学中教师应根据学生的实际情况有选择有侧重地教授，尤其是前面几个介绍基础知识的章节应有所选择。

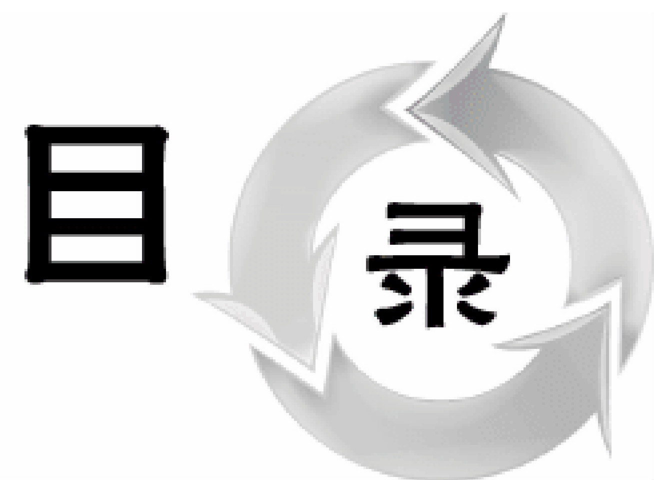
按公安部的教学大纲要求，本课程参考学时为32学时左右，实验占一半的学时，由于总学时的限制，本课程中的基础性实验可有选择地做一些，应突出强调网络安全的专业特色。

本书在编写过程中参考了大量的相关资料，这些资料已列入书后的参考文献中，这里对这些资料的作者表示深深的感谢！

由于编者水平有限，加之时间仓促，本书中难免会有错误，恳请读者予以批评指正，以便进一步改正与完善。

编　者

2012年3月


目
录

# 第 1 章 计算机网络概述

## 1.1　计算机网络的定义

随着计算机和通信技术的发展，网络已经悄然触及人类生活的各个方面，从大型企业的Intranet 到公安部门的金盾网，从连接广泛的 Internet 到小范围的局域网，从普通民众的娱乐生活到科研人员的交流，这些活动无不和网络联系在一起。

网络也为人们提供了极大的方便，人们利用网络可以浏览新闻，收发 E-mail，即时通信，文件传输，远程登录，实时会议服务等，不胜枚举。那么，什么是计算机网络呢?

我们来看两个例子。你在家里使用一台计算机，通过网线连接到 ADSL 调制解调器上，又通过电话线连接到中国联通的网络中去，然后你使用宽带拨号软件(Point to Point Protocol over Ethernet，PPPOE 协议)，输入用户名和密码，就可以连接到 Internet 网络了，这是我们常见的一种上网方式。又如使用手机，通过无线电连接到运营商中国移动的网络中，你可以浏览 WAP 网页，也可以通过手机 QQ 和好友进行即时聊天。通过以上两个例子我们可以看出网络中首先需要有独立计算设备，如计算机、手机、PDA、上网本等；还需要网线、电话线、无线电波、红外线等传输介质，通过它们把计算设备连接起来；连接的过程中你需要使用一个协议进行网络通信，如 PPPOE 协议；网络还需要网络设备，如调制解调器等；我们连接到网络的目的就是要利用网络上的资源，如浏览网页，即时通信等。所以，计算机网络可以这样来定义：计算机网络是利用通信线路和通信设备，把地理上分散的并且有独立功能的计算机连接起来，按照网络协议进行数据通信，实现网络资源共享的计算机的集合。它指出网络是以远程通信和资源共享为目的，其中包括了大量分散而又互联的具有独立功能的计算设备。

## 1.2　计算机网络的产生和发展

计算机网络最早出现于 20 世纪 50 年代，最早的计算机网络是通过通信线路将远方终端资料传送给主计算机处理，这样形成一种简单的联机系统。纵观计算机网络的发展历史可以发现，它和其他事物的发展一样，也经历了从简单到复杂，从低级到高级的过程。在这一过程中，计算机技术与通信技术紧密结合，相互促进，共同发展，最终产生了计算机网络。

### 1.2.1　面向终端的计算机网络

第一代网络是面向终端的计算机网络。1946 年，世界上第一台数字计算机(Electronic Numerical Integrator And Computer，ENIAC)问世，但当时计算机的数量非常少，且非常昂贵。而通信线路和设备的价格相对便宜，当时很多人很想使用位于远端的计算机资源。

20 世纪 50 年代初，美国研制出了一个半自动地面防御系统(Semi-Automatic Ground Environment，SAGE)，边境上的警戒雷达可将空中飞机的方位、距离和高度等信息通过通信线路传到北美防空司令部信息中心的大型计算机进行处理。这种将计算机与通信线路相连的举措是一个创举，是计算机网络发展史上的一个里程碑。

在 SAGE 的基础上，人们把多台终端连接到计算机上，形成如图 1-1(a)所示的连接形式，终端不是独立的计算机，它只有键盘和显示器，没有 CPU 和内存，只负责输入输出，主计算机负责数据的处理与存储。所以这一时期的网络不是真正意义上的计算机网络，而只是计算机网络的一个雏形。

随着终端数量的日益增多，这种结构系统的缺点也逐渐显露出来：主计算机需要处理每台终端的输入输出，负担明显过重；每个终端都有线路连接到主机，线路的利用率低。为了提高线路的利用率和减轻主机的负担，在通信系统中使用了集中器和前端机(Front End Processor，FEP)，如图 1-1(b)所示。集中器把多个终端连接起来通过一条线路连接到主机上，前端处理机在主机的前端负责处理通信功能，减轻了主机的负担。联机终端网络典型的范例是美国航空公司与 IBM 公司在 20 世纪 60 年代投入使用的飞机订票系统(Semi-Automatic Business-Research Environment，SABRE-I)，它由一台计算机和全美范围内 2000 个终端组成。

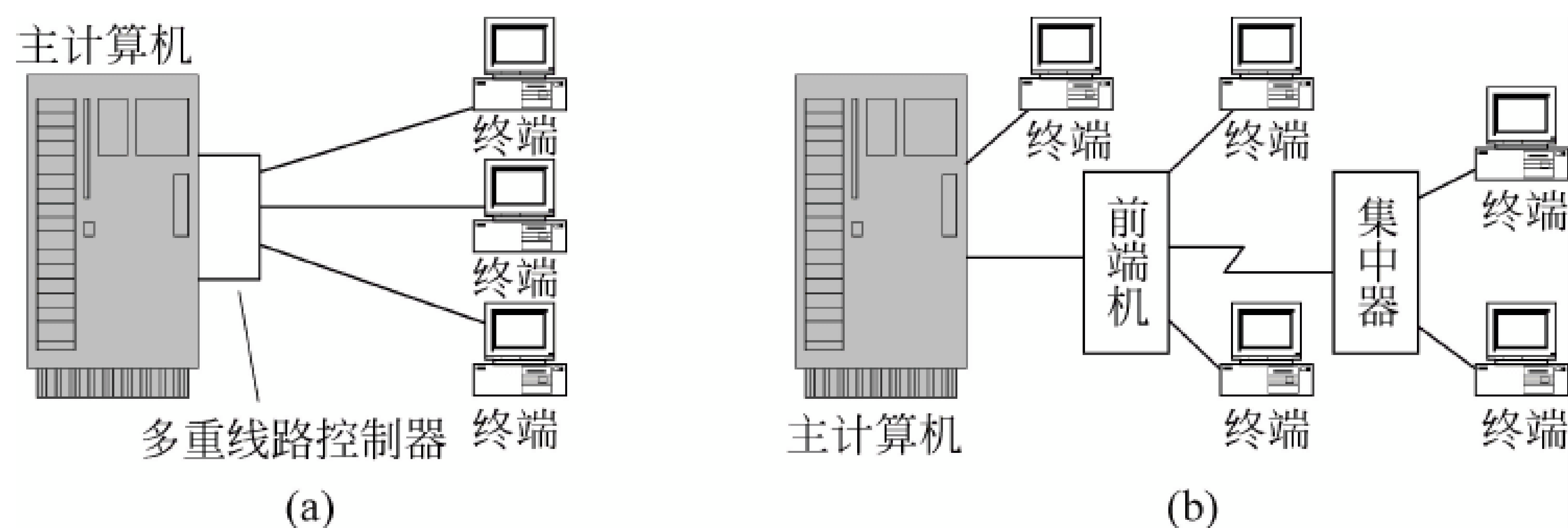



图 1-1　具有通信功能的单机系统

### 1.2.2　计算机通信网络

为了克服第一代计算机网络的缺点，提高网络的可靠性和可用性，人们开始研究将多台计算机相互连接的方法。第二代网络是从 20 世纪 60 年代中期到 70 年代中期，随着计算机技术和通信技术的进步，已经形成了将多个主机相互连接起来，以多处理机为中心的网络，并利用通信线路将多台主机连接起来，为终端用户提供服务。

第二代网络是在计算机网络通信网的基础上通过完成计算机网络体系结构和协议的研究，形成的计算机初期网络。如20世纪60至70年代初期由美国国防部高级研究计划局研制的ARPANET网络，它将计算机网络分为资源子网和通信子网。

这一时期网络具有以下特点：

(1) 采用以程控交换为基础的分组交换技术。

(2) 以远程数据传输和信息共享为主要目的。

(3) 采用了层次结构的网络体系结构模型与协议体系。

(4) 把网络分为资源子网和通信子网。

### 1.2.3 开放式的标准化计算机网络

20世纪80年代是计算机局域网络的发展和盛行时期。当时采用的是具有统一的网络体系结构并遵守国际标准的开放式和标准化的网络，它是网络发展的第三代。

20世纪70年代出现个人计算机(Personal Computer，PC)，随着性能不断提高，价格不断下降，个人计算机从“神坛”走入寻常百姓生活，从科学计算走入了事务处理。PC走入工厂、商店、学校、甚至家庭，人们把一栋楼、一个单位的计算机连接起来形成一个局域网(Local Area Network，LAN)。计算机网络得到迅速的发展和广泛的应用。

在第三代网络出现以前网络是无法实现不同厂家设备互连的，早期，各厂家为了霸占市场，各厂家采用自己独特的技术并开发了自己的网络体系结构，当时，IBM发布的系统网络体系结构(System Network Architecture，SNA)和DEC公司发布的数字网络体系结构(Digital Network Architecture，DNA)。不同的网络体系结构是无法互连的，所以不同厂家的设备无法达到互连，即使是同一家公司不同时期的产品也是无法互连的，这样就阻碍了大范围网络的发展。后来，为了实现网络大范围的发展和不同厂家设备的互连，1977年国际标准化组织(International Organization for Standardization，ISO)提出一个标准框架——开放系统互连参考模型(Open System Interconnection/Reference Model，OSI/RM)。1984年正式发布了OSI，使厂家设备、协议达到全网互联。

OSI/RM参考模型把网络分为七个层次，并规定，计算机之间只能在对应层之间进行通信，大大简化了网络通信原理，是公认的新一代计算机网络体系结构的基础。

### 1.2.4 综合、智能、高速的互联网络

随着数字通信的出现和光纤的接入，网络进入高速互联时代即第四代计算机网络时代。与第三代网络相比，其特点是：高速化、综合化、计算机协同能力。

通常意义上的计算机互联网是以电信网作为信息的载体的，计算机通过电信网中的X.25网，DDN网、帧中继网等传输数据。随着因特网的发展，人们对网络提出了更高的要求，人们希望通过互联网进行视频会议，进行远程教学，看高清电视，甚至实现电信网、有线电视网和计算机网“三网合一”。对互联网的主干网进行了升级改造，波分复用技术已把网

速提升到400Gb/s，IP over ATM，IP over SDH，IP over WDM等技术也开始使用。

光纤等高速传输介质和高速网络技术带来了更高的传输速率，快速交换技术保证了更低的延时。网络中多种媒体(语音、视频、图像、数据等)的出现使业务出现了综合化的趋势。

### 1.2.5 网络时代的三大定律

微电子技术是信息产业发展的基础，微电子技术的发展可以用摩尔定律来描述，即微电子芯片的计算能力每18个月提高一倍，10年翻100倍。自1980年以来，微处理器的速度一直以每5年10倍的速度增长。到2020年之前集成电路仍将按摩尔定律高速发展。预测到2018年，高性能CPU芯片上可集成的晶体管数将超过2560亿个。多核通用CPU利用摩尔定律延续带来的片上海量晶体管资源来集成多个处理器核以提升性能，成为当前高性能通用CPU的发展趋势，片上集成的处理器核数目每两年翻一番(摩尔定律的新解释)。

在网络领域有光纤定律，又称超摩尔定律：骨干网带宽每9个月翻番，10年翻10 000倍，带宽需求呈超高速增长的趋势。今天，几乎所有知名的电信公司都在乐此不疲地铺设缆线。当带宽变得足够充裕时，上网的代价也会下降。

麦特卡尔夫定律：以太网的发明人鲍勃·麦特卡尔夫告诉我们，网络价值同网络用户数量的平方成正比(即$N$个连接能创造$N^2$的效益)。如果将机器连成一个网络，在网络上，每一个人可以看到所有其他人的内容，100人每人能看到100人的内容，所以效率是10 000。10 000人的效率就是100 000 000！用户决定互联网公司的存亡，因此，互联网公司拼命地圈人。一个互联网公司可以圈到几乎是一个行业的用户，所以个别的互联网公司的创立者或投资者可以成就几十亿，几百亿的财富。

### 1.2.6 网络的发展趋势

**1. 从IPv4过渡到IPv6**

现在普遍使用的技术是IPv4，IPv4技术在地址空间上存在很大的局限性，此外，它还在服务质量、传送速度、安全性、支持移动性与多播等方面也有局限性，这些局限性妨碍网络的发展，使许多服务与应用难以开展。因此，网络技术势必过渡到IPv6技术，IPv6技术除了从根本上解决地址短缺问题外，还会提高网络吞吐量，改善服务质量，提高安全性，支持即插即用和移动性，更好地实现多播功能等。IPv6将使网络上升到一个新台阶，并将在发展过程中不断地完善。

**2. 业务综合化**

将来的计算机网络不仅可以提供数据通信和数据处理业务，而且还可提供声音、图形、图像等通信和处理业务，即业务综合化。业务综合化要求网络支持所有的不同类型和不同速率的业务，如话音、传真等窄带业务；广播电视、高清晰度电视等分配型宽带业务；可视电话、交互式电视、视频会议等交互型宽带业务；高速数据传输等突发型宽带业务等。为了满足这些要求，计算机网络需要有很高的速度和很宽的频带。

**3. 3G 以上的移动通信系统飞速发展**

3G 以上包括 3G、4G 乃至 5G 系统。3G 以上技术正在国内大范围地应用，它比以前应用的 2G 和 2.5G 系统传输容量更大，灵活性更高。它以宽带多媒体技术为基础，使用更高更宽的频带，能够在不同网络之间无缝连接，提供满意的服务。

**4. 三网融合**

为了实现全面互联，共享信息资源，近期要实现“三网”互联，即“三网合一”，三网是指电信网、广播电视网、计算机网。三网互联指将三种网络相互渗透、互相兼容，并逐步整合成为统一的现代信息通信网络。现在，我国已经在多地开始“三网合一”的试验，“三网合一”的困难不在于技术，而在于利益如何分配。

**5. 物联网将飞速发展**

物联网(Internet of Things，IOT)通过传感器、射频识别技术、全球定位系统等技术，实时采集任何需要监控、连接、互动的物体或过程，采集各种需要的信息，通过各类可能的网络接入，实现物与物、物与人的泛在链接，实现对物品和过程的智能化感知、识别和管理。

物联网是继计算机互联网之后世界信息产业发展的第三次浪潮，是网络在业务和应用领域的拓展。它主要利用了 RFID、无线数据通信技术，把感应器嵌入到各种物体中，然后将物联网与现有的互联网整合起来，实现人类社会与物理系统的整合，以实施对各种物体的管理和控制。可以预见，物联网的来临，必将给人类社会带来翻天覆地的变化。

## 1.3　计算机网络的主要功能

组建计算机网络的目的就是要实现计算机网络的基本功能。

**1. 资源共享**

1) 硬件资源的共享

计算机网络上正在使用着各种硬件资源，如巨型计算机、专用的高性能计算机、大容量存储设备、高性能打印机、高精度图形设备等。用户可以使用网络中任意一台计算机所附接的硬件设备，例如登录到一台大型的高性能计算机，利用它的超级处理能力，进行科学计算；使用网络中的网络打印机完成打印作业；利用网络中的网络存储设备存储文件等。

2) 软件资源的共享

用户可以使用远程主机的软件(系统软件和应用软件)，既可以将相应软件调入本地计算机执行，也可以将数据送至对方主机，运行软件，并返回结果。

3) 数据共享

网络用户可以使用其他主机和用户的数据。数据共享是资源共享中最常见的方式。

**2. 数据通信**

通过网络用户可以进行数据通信，比如：通过电子邮件及时快捷地把信息发给了同学；通过 QQ、MSN 等即时通信软件和朋友进行即时的音频、视频聊天；利用 CUTFTP 等文件

传输软件进行文件上传和下载；通过网络使用 IP 电话和家人进行电话沟通等这些都是网络数据通信的实例。

**3. 实现分布式计算**

由于计算机网络的出现，使分布式计算成为可能。一个大的计算任务，把任务分解并分配到不同计算机上进行计算，最后再把结果综合起来。目前常见的分布式计算项目通常使用世界各地成千上万志愿者计算机的闲置计算能力，通过互联网进行数据传输。有分析地外无线电信号，从而搜索地外生命迹象的 SETI@home 项目，该项目数据基数很大，超过了千万位数，是目前世界上最大的分布式计算项目，已有一百六十余万台计算机加入了此项目。也有分析计算蛋白质的内部结构和相关药物的 Folding@home 项目，该项目大约有十万余志愿者参加(在中国内地大约有 6000 位志愿者)。这些项目很庞大，需要惊人的计算量，由一台计算机计算是不可能完成的。

**4. 提高计算机的可靠性**

一方面，通过计算机网络系统的差错控制机制保证数据的正确无误。另一方面，网络中各计算机还可以通过网络成为彼此的后备机，从而增强了系统的可靠性。

**5. 均衡负载互相协作**

负载平衡是指工作被均匀地分配给网络上的各台计算机。网络控制中心负责分配和检测，当某台计算机负载过重时，系统会自动转移部分工作到负载较轻的计算机中去处理。

## 1.4 计算机网络的拓扑结构

计算机网络的连线方式千变万化，为了研究网络而抛开网络线缆的物理连接来讨论网络系统的连接形式，研究网络线缆构成的几何形状，这叫做网络的拓扑结构。它能从逻辑上表示出网络服务器、工作站的网络配置和互相之间的连接。常见的网络拓扑结构有总线型、星型、树型、环形、混合型等拓扑结构。

### 1.4.1 总线型拓扑结构

总线型拓扑结构(图 1-2)采用单根数据传输线作为通信介质，所有的站点都通过相应的硬件接口直接连接到通信介质，而且能被所有其他的站点接受。总线型网络结构中的节点为服务器或工作站，通信介质为同轴电缆。

由于所有的节点共享一条公用的传输链路，所以一次只能由一个设备传输。这样就需要某种形式的访问控制策略，来决定下一次哪一个节点可以发送。一般情况下，总线型网络采用载波监听多路访问/冲突检测(Carrier Sense Multiple Access/Collision Detect，CSMA/CD)控制策略。

总线型拓扑结构在局域网中得到广泛的应用，主要优点有：

(1) 布线容易、线缆用量最短。总线型网络中的节点都连接在一个公共的通信介质上，

所以需要的线缆长度最短，减少了安装费用，易于布线和维护。

(2) 可靠性高。总线结构简单，从硬件观点来看，十分可靠。

(3) 易于扩充。在总线型网络中，如果要增加长度，可通过中继器加上一个附加段；如果需要增加新节点，只需要在总线的任何点将其接入。

(4) 易于安装。总线型网络的安装比较简单，对技术要求不是很高。

总线型拓扑结构虽然有许多优点，但也有自己的局限性：

(1) 故障诊断困难。虽然总线拓扑简单，可靠性高，但故障检测却不容易。因为具有总线拓扑结构的网络不是集中控制，故障检测需要在网上各个节点进行。

(2) 故障隔离困难。对于介质的故障，不能简单地撤销某工作站，这样会切断整段网络。

(3) 中继器配置。在总线的干线基础上扩充时，可利用中继器，需要重新设置，包括电缆长度的裁剪、终端匹配器的调整等。

(4) 通信介质或中间某一接口点出现故障，整个网络随即瘫痪。

(5) 终端必须是智能的。因为接在总线上的节点有介质访问控制功能，因此必须是智能的，从而增加了站点的硬件和软件费用。

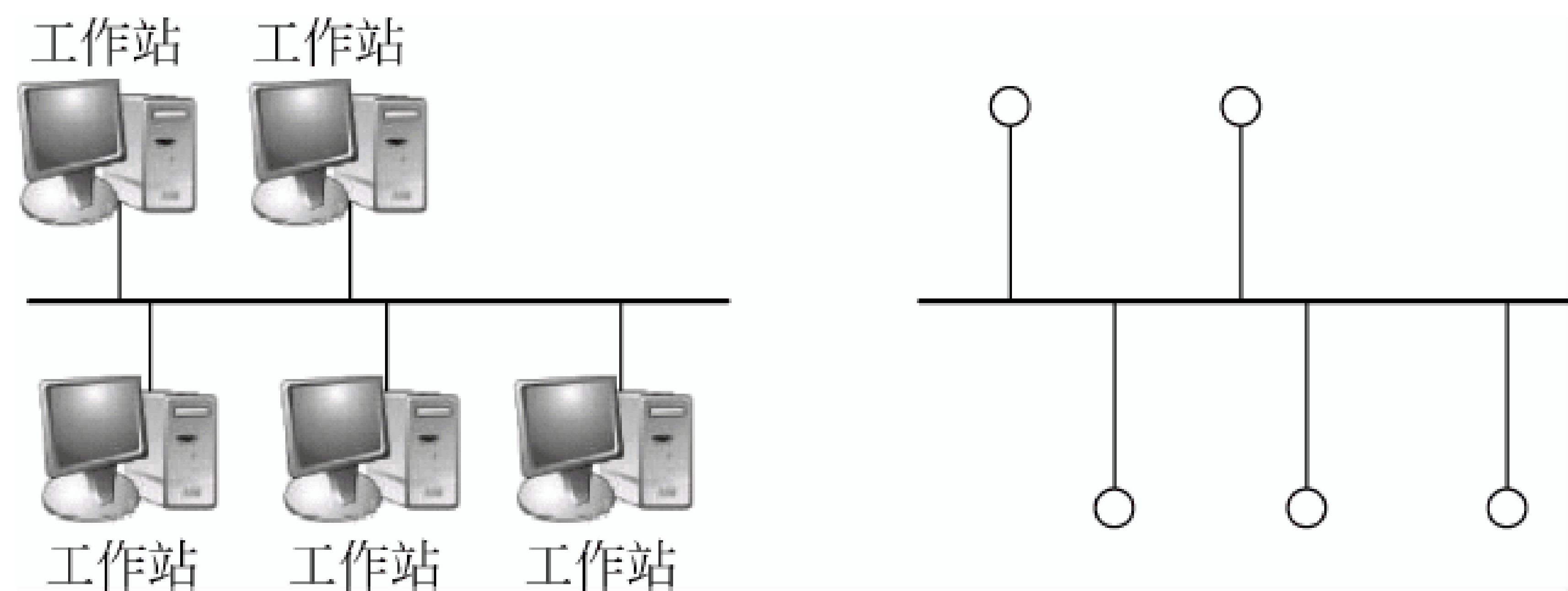



图 1-2　总线型拓扑结构

## 1.4.2　星型拓扑结构

星型拓扑结构(图 1-3)是由中央节点和通过点到点链路连接到中央节点的各节点组成。这种结构以中央节点为中心，因此又称为集中式网络。工作站到中央节点的线路是专用的，不会出现拥挤的瓶颈现象。

星型拓扑结构中，中央节点为集线器(Hub)，其他外围节点为服务器或工作站；通信介质为双绞线或光纤。

星型拓扑结构被广泛地应用于网络中智能主要集中于中央节点的场合。由于所有节点的往外传输都必须经过中央节点来处理，因此，对中央节点的要求比较高。

星型拓扑结构信息发送的过程为：某一工作站有信息发送时，将向中央节点申请，中央节点响应该工作站，并将该工作站与目的工作站或服务器建立会话。此时，就可以进行无延时的会话了。

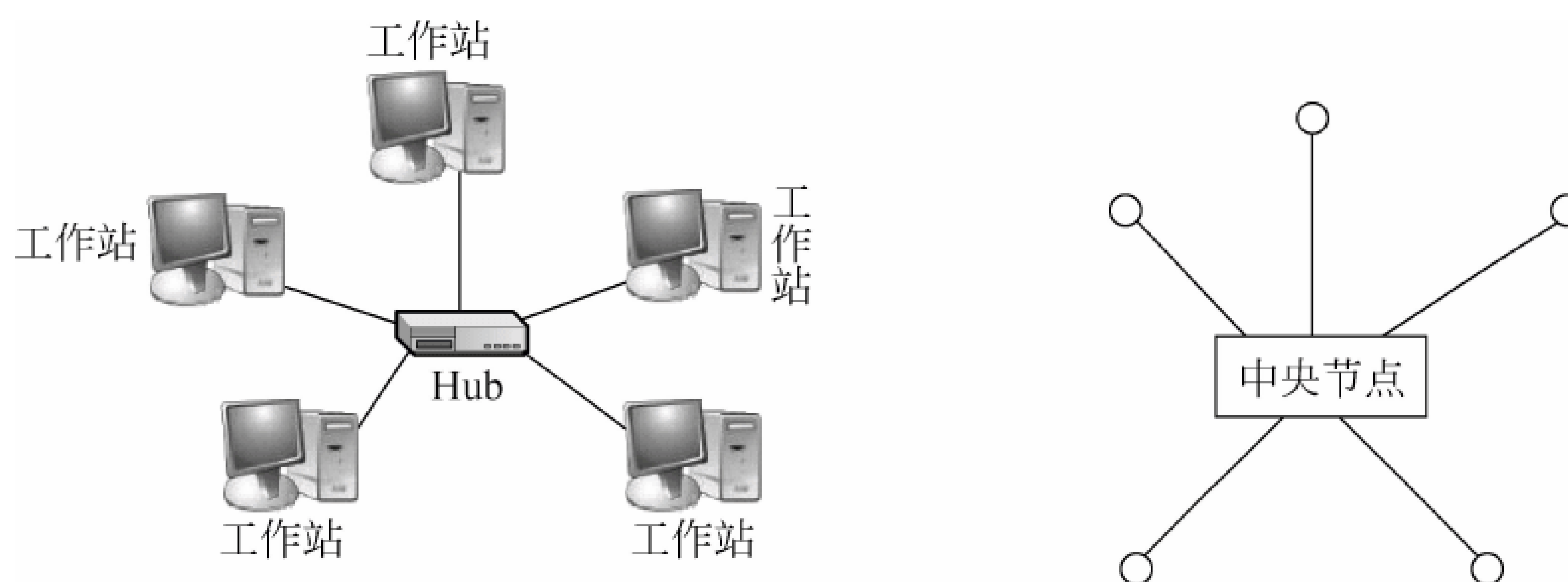



图 1-3　星型拓扑结构

星型拓扑结构的优点为：

(1) 可靠性高。在星型拓扑的结构中，每个连接只与一个设备相连，因此，单个连接的故障只影响一个设备，不会影响全网，也消除了数据传输过程中的堵塞现象。

(2) 易于建网，易于管理。每一节点独占一条传输线路，便于在网络中增加新的节点。

(3) 故障诊断容易。如果网络中的节点或者通信介质出现问题，只会影响到该节点或者通信介质相连的节点，不会涉及整个网络，从而比较容易判断故障的位置。

星型拓扑结构虽有许多优点，但也有缺点：

(1) 对中央节点的依赖性强。星型拓扑结构网络中的外围节点对中央节点的依赖性强，如果中央节点出现故障，则全部网络不能正常工作。

(2) 扩展困难、安装费用高。增加网络新节点时，无论有多远，都需要与中央节点直接连接，布线困难且费用高。

### 1.4.3 环型拓扑结构

环型网络(图 1-4)中各节点通过环路接口连在一条首尾相连的闭合环型通信线路中，环路上任何节点均可以请求发送信息。请求一旦被批准，便可以向环路发送信息。环型网中的数据可以是单向传输也可以是双向传输。由于环线公用，一个节点发出的信息必须穿越环中所有的环路接口，信息流中目的地址与环上某节点地址相符时，信息被该节点的环路接口所接收，而后信息继续流向下一环路接口，一直流回到发送该信息的环路接口节点

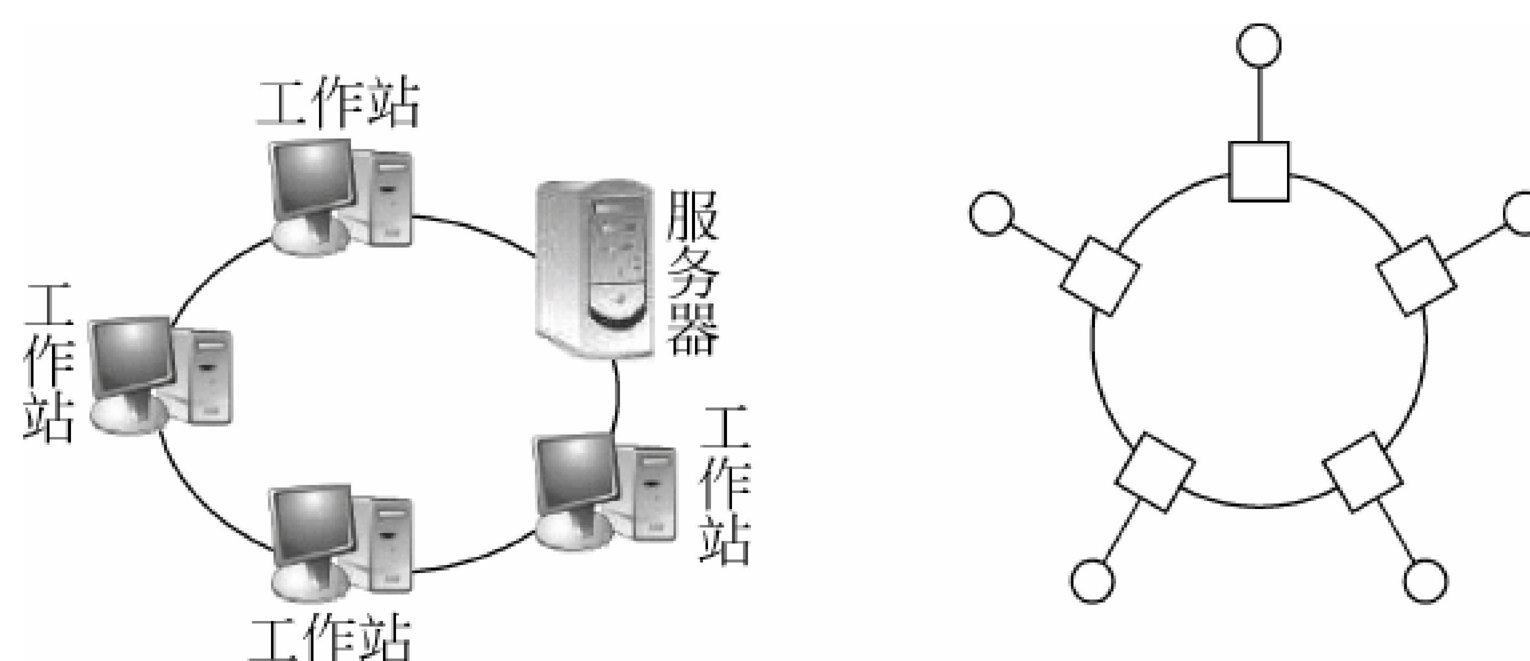



图 1-4　环型拓扑结构图

为止。

环形拓扑结构的优点：

(1) 信息在网络中沿固定方向流动，两个节点间仅有唯一的通路，大大简化了路径选择的控制。

(2) 电缆长度短。环形拓扑网络所需的电缆长度和总线拓扑网络相似，但比星型拓扑网络要短得多。

(3) 可使用光纤。光纤的传输速率很高，十分适合于环形拓扑的单方向传输。

环形拓扑的缺点：

(1) 节点的故障会引起全网故障。因为环上的数据传输要通过接在环上的每一个节点，一旦环中某一节点发生故障就会引起全网的故障。

(2) 故障检测困难。这与总线拓扑相似，因为不是集中控制，故障检测需在网上各个节点进行，因此就不是很容易。

(3) 环形拓扑结构的媒体访问控制协议都采用令牌传递的方式，在负载很轻时，信道利用率相对来说就比较低。

(4) 由于信息是串行穿过多个节点环路接口，当节点过多时，影响传输效率，使网络响应时间变长。

(5) 由于环路封闭故扩充不方便。

### 1.4.4　树型拓扑结构

树型结构(图 1-5)是总线型结构的扩展，它是在总线网上加上分支形成的，其传输介质可有多条分支，但不形成闭合回路，树型网是一种分层网，其结构可以对称，联系固定，具有一定容错能力，一般一个分支和节点的故障不影响另一分支节点的工作，任何一个节点送出的信息都可以传遍整个传输介质，也是广播式网络。一般树型网上的链路相对具有一定的专用性，无须对原网做任何改动就可以扩充工作站。

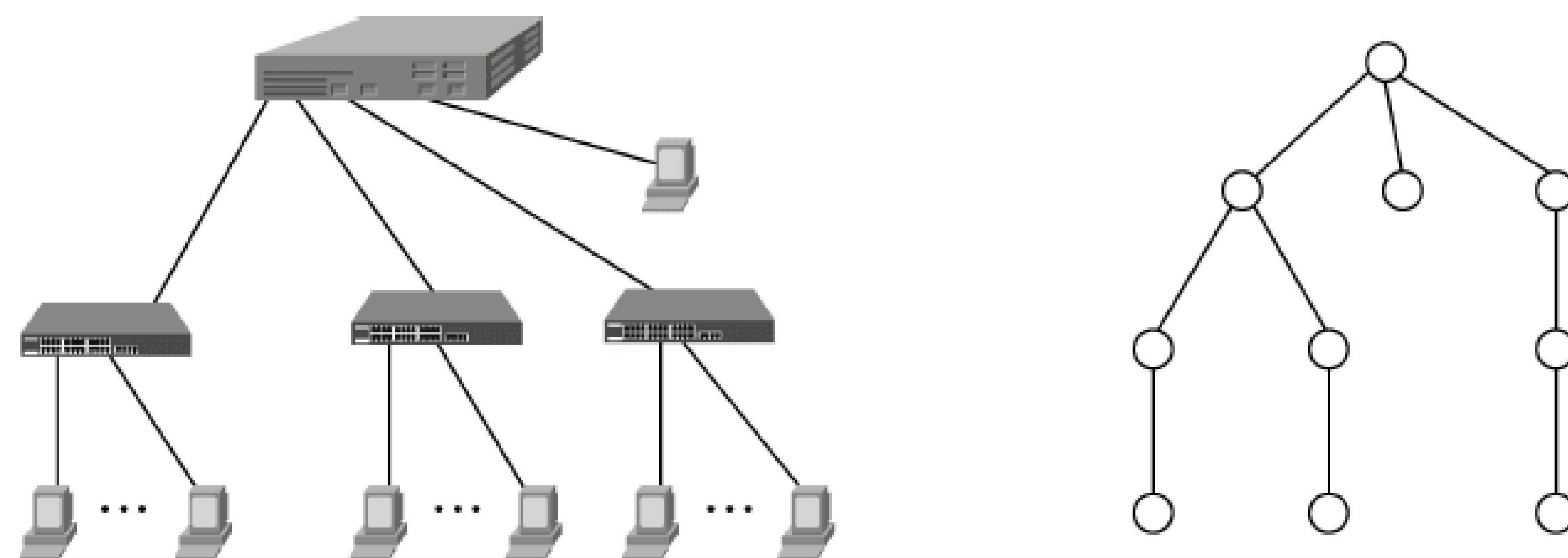



图 1-5　树型拓扑结构

树型拓扑的优点：

(1) 易于扩展。这种结构可以延伸出很多分支和子分支，这些新节点和新分支都能容易地加入网内。

（2）故障隔离较容易。如果某一分支的节点或线路发生故障，很容易将故障分支与整个系统隔离开来。

树型拓扑的缺点：

各个节点对根的依赖性太大。如果根发生故障，则全网不能正常工作。从这一点来看，树型拓扑结构的可靠性有点类似于星型拓扑结构。

### 1.4.5 网状拓扑结构

网状拓扑结构（图 1-6）的网络由分布在不同地理位置的计算机经传输介质和通信设备连接而成。在网状拓扑结构中，节点之间的连接是任意的、无规律的且每两个节点之间的通信链路可能有多条。因此，必须使用“路由选择”算法进行路径选择。这种结构在广域网中得到了广泛的应用，它的优点是不受瓶颈问题和失效问题的影响。由于节点之间有许多条路径相连，可以为数据流的传输选择适当的路由，从而绕过失效的部件或过忙的节点，因此，系统的安全性高。这种结构虽然比较复杂，成本也比较高，提供上述功能的网络协议也较复杂，但由于它的可靠性高，仍然受到用户的欢迎。

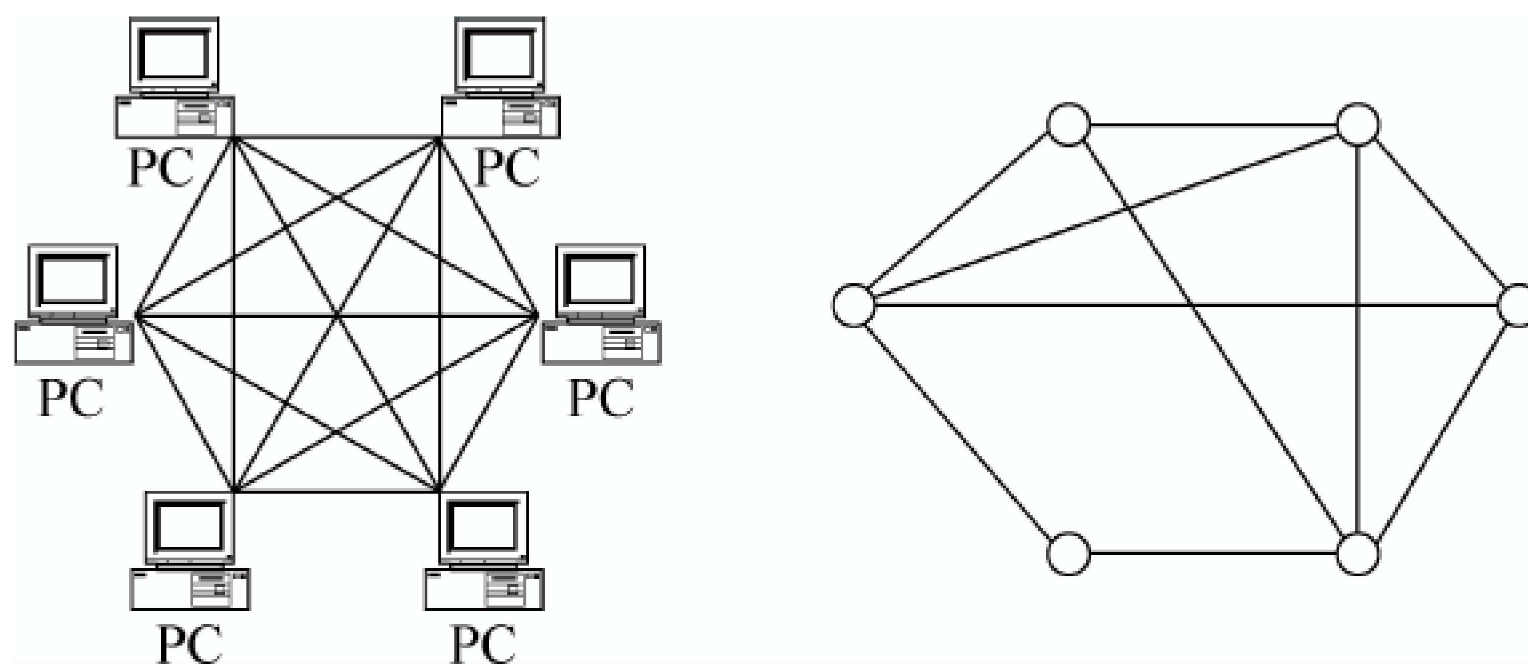



图 1-6 网状拓扑结构图

### 1.4.6 混合型拓扑结构

混合型网络拓扑结构是指多种结构（如星型结构、环形结构、总线型结构）单元组成的结构，但常见的是由星型结构和总线型结构组合而成。混合型网络拓扑结构更能满足较大网络的拓展，解决星型网络在传输距离上的局限，而同时又解决了总线型网络在连接用户数量的限制。

混合型拓扑结构的优点：

（1）应用广泛。这主要是因它解决了星型和总线型拓扑结构的不足，满足了较大单位组网的实际需求。目前在一些智能化的信息大厦中的应用非常普遍。在一幢大厦中，各楼层间采用光纤作为总线传输介质，一方面可以保证网络传输距离，另一方面，光纤的传输性能要远好于同轴电缆，所以，在传输性能上也给予了充分保证。各楼层内部仍普遍采用使用双绞线星型以太网。

(2) 扩展灵活。这主要是继承了星型拓扑结构的优点。但由于仍采用广播式的消息传送方式,所以在总线长度和节点数量上也会受到限制,不过在局域网中的影响并不是很大。

混合型拓扑结构的缺点如下:

(1) 性能差。因为其骨干网段采用总线网络连接方式,所以各楼层和各建筑物之间的网络互联性能较差。另外,这种结构网络具有总线型网络结构的弱点,网络速率会随着用户的增多而下降。当然在采用光纤作为传输介质的混合型网络中,这些影响还是比较小的。

(2) 较难维护。这主要受到总线型网络拓扑结构的制约,如果总线出现故障,则整个网络也就瘫痪了,但是如果是分支网段出了故障,则不影响整个网络的正常运作。再一个就是整个网络非常复杂,维护起来不容易。

# 1.5　计算机网络的分类

计算机网络分类方式多种多样,可以按地理范围、拓扑结构、传输速率和传输介质来分类。

## 1.5.1　按地理范围分类

网络中计算机设备之间的距离可近可远,即网络覆盖地域面积可大可小。按照联网的计算机之间的距离和网络覆盖面的不同,一般分为局域网、城域网和广域网。

**1. 局域网**

局域网(LAN)是将较小地理范围内的计算机或数据终端连接起来的通信网络。局域网的覆盖范围较小,一般是在几十米到几千米的范围之间。常用于办公室、楼宇、楼群、校园或企业等小范围内,连接的计算机及其他设备数量从几台到几千台不等。

局域网具有以下特征:

(1) 覆盖的地理范围有限,一般在几千米以内,适用于某一部门或某一单位。

(2) 传输速率高、误码率低:局域网内的传输速率一般为 10Mb/s 或 100Mb/s,甚至可达 1000Mb/s。

(3) 组网简单、成本低、使用方便灵活。

(4) 决定局域网特性的主要技术要素为网络拓扑、传输介质与介质访问方法,按介质访问方法进行分类,局域网可分为共享式局域网和交换式局域网。

**2. 广域网**

广域网(Wide Area Network,WAN)也称远程网,范围在几十千米到几千千米,覆盖一个国家、一个地区,甚至全世界。广域网的通信子网可以利用公用分组交换网、卫星通信网和无线分组交换网,将分布在不同地区的局域网或计算机系统互连起来,达到资源共享的目的。广域网应具有以下特点:

(1) 适应大容量与突发性通信的要求。

(2) 适应综合业务服务的要求。

(3) 开放的设备接口与规范化的协议。

(4) 完善的通信服务与网络管理。

**3. 城域网**

城域网(Metropolitan Area Network,MAN)是介于广域网与局域网之间的一种高速网络。它的覆盖范围一般为几千米到几万米,将一个城市内的大量企业、机关、公司、学校与其他社会团体的不同计算机网络连接起来实现多用户、多信息传输的综合信息网络。

## 1.5.2 其他网络分类

**1. 按传输速率分类**

网络的传输速率有快有慢,传输速率快的称高速网,传输速率慢的称低速网。传输速率的单位是 b/s(每秒比特数,英文缩写为 bps)。一般将传输速率在 Kb/s~Mb/s 范围的网络称低速网,在 Mb/s~Gb/s 范围的网称高速网。也可以将 Kb/s 网称低速网,将 Mb/s 网称中速网,将 Gb/s 网称高速网。

网络的传输速率与网络的带宽有直接关系。带宽是指传输信道的宽度,带宽的单位是 Hz(赫兹)。按照传输信道的宽度可分为窄带网和宽带网。一般将 kHz~MHz 带宽的网称为窄带网,将 MHz~GHz 的网称为宽带网,也可以将 kHz 带宽的网称窄带网,将 MHz 带宽的网称中带网,将 GHz 带宽的网称宽带网。通常情况下,高速网就是宽带网,低速网就是窄带网。

**2. 按传输介质分类**

传输介质是指数据传输系统中发送装置和接收装置间的物理媒体,按其物理形态可以划分为有线和无线两大类。

1) 有线网

传输介质采用有线介质连接的网络称为有线网,常用的有线传输介质有同轴电缆、双绞线和光导纤维。

2) 无线网

采用无线介质连接的网络称为无线网。目前无线网主要采用三种技术:微波通信,红外线通信和激光通信。这三种技术都是以大气为介质的。其中微波通信用途最广,这部分内容将在 3.3 节中介绍。

**3. 按拓扑结构分类**

按网络的拓扑结构可以分为:总线型网络、星型拓扑结构、树型拓扑结构、环形拓扑结构、网状拓扑结构等。上文已有介绍这里不再赘述。

**4. 按网络的所有权分类**

1) 公用网络

一般由国家或电信企业组建、管理和控制的通信网络,可为国内的任何部门或个人提供

有偿服务。如CHINANET、CERNET等。

2）专用网络

专用网络是某部门为特殊需求而建造的计算机网络，该网络不向专用网络以外的人提供服务。如军队专用的长城网、公安专用的金盾网以及铁路、电力、银行等部门也都拥有各自的专用网络。

**5. 按服务类型分类**

1）对等网络

网络中没有服务器，网络中所有的计算机都处于平等的地位。

2）基于服务器的网络

在网络中用性能较强、拥有特定资源的计算机作为服务器，服务器为其他客户机提供服务。客户机运行客户端软件，向服务器提出服务请求。

**6. 按照通信信道的类型分类**

1）广播式网络

广播式网络中所有节点使用一个公共的通信信道，在任一时刻只允许一个节点使用公共信道，一个节点利用信道"传送"数据时，其他节点只能处于"收听"状态。在这种网络中，需要解决以下问题：①由谁来传送信息；②在公共信道发生冲突时如何解决冲突。常见的广播式网络有总线型网络、无线网络和卫星通信网络。

网络中的每个节点在接收到信息后，都会把信息中的目标地址与自己的地址相比较，若地址相同，则接收并处理信息，否则丢弃信息。在广播式网络中，信息在一个源节点和一个目标节点之间传递，这种方式叫单播；一个节点发出信息后，所有其他节点都接收并处理这些信息，这种方式叫广播；把信息发给网络中的多个而非网络中的所有节点，这种方式叫组播。

2）点对点的通信网络

在点对点的通信网络中，两个节点直接相连，或通过其他节点相连，每个节点与其他节点通信时，不会产生冲突。在通过其他节点相连的点对点通信网络中可能存在多条路径，因此必须解决路径的选择问题。常见的点对点通信网络有星型网络、环形网络、树型网络和网状网络。

## 1.6 计算机网络的组成

从资源构成的角度来看，计算机网络由网络硬件和网络软件组成，如图1-7所示。

### 1.6.1 网络硬件资源

计算机网络硬件是网络的基础，主要包括计算机、网络设备、传输介质等。

**1. 计算机**

这里讲的计算机并非传统意义上的计算机,而是指具有数据处理和网络功能的计算设备。可以是大型机、中型机、小型机、工作站、微机、平板电脑、PDA、手机等移动计算设备。它们通过有线或无线传输介质接入到网络,实现网络功能。

**2. 网络设备**

常见的网络设备包括:网卡、调制解调器、集线器、中继器、网桥、交换机、路由器、网关。

**3. 传输介质**

传输介质是指网络中信息传输的物理通道。常见的传输介质分为有线传输介质和无线传输介质,有线介质有:同轴电缆、双绞线、光纤。无线传输介质有:无线电、微波、激光、红外线、卫星通道等。

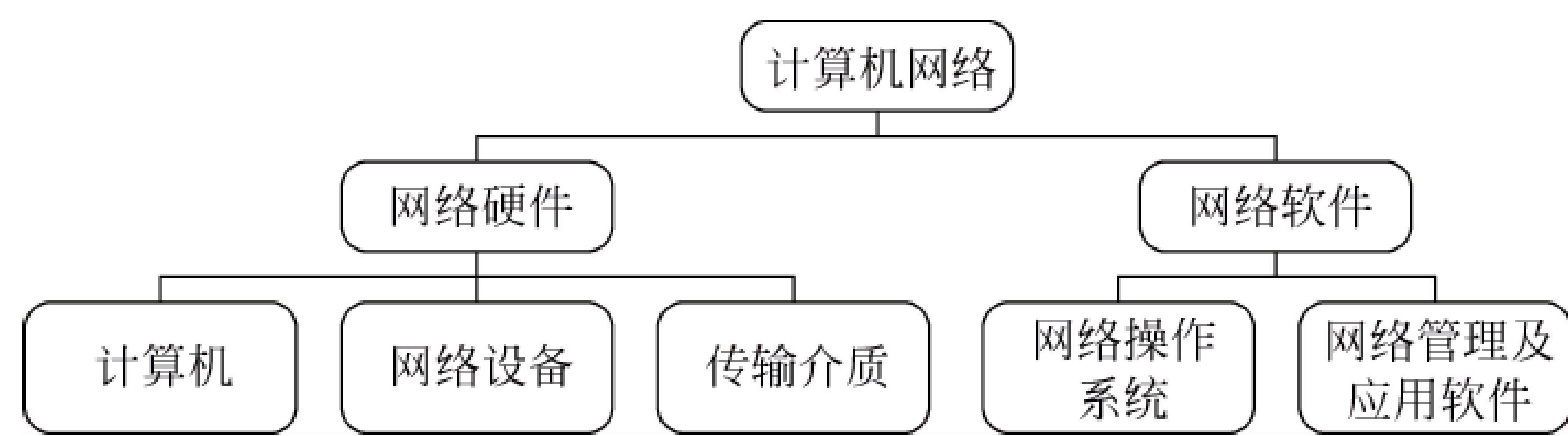



图 1-7 计算机网络的组成

## 1.6.2 网络软件资源

为了充分利用及管理各种网络资源,并采取一系列安全措施,防止用户对数据的不合理利用甚至是丢失和破坏,我们需要管理各种网络资源的软件。主要包括:

(1) 网络操作系统。网络操作系统主要是实现网络资源的管理与分配,以实现网络资源的共享。

(2) 网络管理与应用软件。网络管理软件是对网络资源进行监控管理并对网络进行维护的软件。网络应用软件是为网络用户提供服务,解决用户实际问题的软件。

## 1.6.3 资源子网与通信子网

计算机网络从逻辑功能上分为资源子网和通信子网。

资源子网负责全网的数据处理业务,并向网络用户提供各种网络资源和网络服务。资源子网主要包括主机、终端、计算机外设等。主机通过通信线路连接到通信子网中的通信控制处理机上,它拥有各种终端用户访问的资源,负担着数据处理的任务。终端是直接面向用户的交互设备,向网络中的主机提出信息服务的请求。计算机外设包括网络存储设备(如NAS,SAN 等)、高速打印机、大型绘图仪等。

通信子网承担着资源子网的数据传输、转接和变换等通信处理工作。通信子网常由通信控制处理机、通信线路与其他通信设备组成。通信控制处理机一方面作为资源子网中的

主机、终端接入节点；另一方面它又作为通信子网中的分组存储转发节点，完成分组的接收、校验、存储和转发功能。通信线路是指传输介质，它连接于主机与通信控制处理机之间或通信控制处理机与通信控制处理机之间，主要有双绞线、同轴电缆、光纤、无线电等。

# 思考与练习

**一、填空题**

1. 计算机网络按地理覆盖范围分类，可以分为________、________和________。

2. 网络拓扑结构可分为________、________、________、________、________和________等拓扑结构。

3. 计算机网络按传输介质分为________和________网络。

4. 计算机网络从逻辑功能上分为________子网和________子网。

5. 按网络的所有权分类可分为________网络和________网络。

6. 计算机网络的主要功能包括________、________、________、________和________。

7. 网络易发生"瓶颈"现象的拓扑结构是________。

**二、选择题**

1. 计算机网络是(　　)与计算机技术相结合的产物。

A. 网络技术　B. 通信技术　C. 数据库技术　D. 管理技术

2. 一座大楼内的计算机网络，属于(　　)。

A. WAN　B. LAN　C. MAN　D. PAN

3. 计算机网络按照通信信道的类型分类分为(　　)和(　　)。

A. 通信子网　资源子网　B. 对等网　基于服务器的网络
C. 广播式网络　点对点的通信网络　D. 局域网　广域网

4. 根据网络的地理范围可以分为局域网、城域网和(　　)。

A. Internet　B. LAN　C. WAN　D. MAN

5. 从计算机网络资源构成的角度可以分为网络硬件资源和(　　)。

A. 网络软件资源　B. 数据资源　C. 网络资源　D. 信息资源

6. 当前，局域网中最常见的拓扑结构是(　　)。

A. 总线型拓扑结构　B. 环形拓扑结构
C. 树型拓扑结构　D. 星型拓扑结构

7. 连接到计算机网络上的计算机都是(　　)。

A. 高性能计算机　B. 具有通信能力的计算机
C. 自治计算机　D. 主从计算机

8. 不属于"三网合一"的"三网"是(　　)。

A. 电信网　B. 有线电视网　C. 计算机网　D. 交换网

9. Internet 最先是由美国的(　　)网发展和演化而来。

A. ARPANET　　B. NSFNET　　C. CSNET　　D. BITNET

10. 借用于公用电话网构成的网络一般属于(　　)。

A. 广域网　　B. 局域网　　C. 对等网　　D. 公用网

**三、思考题**

1. 什么是计算机网络,它的主要功能是什么?
2. 计算机网络的发展过程是怎样的,趋势是什么?
3. 计算机网络是由哪些资源组成的,分为哪些子网?
4. 计算机网络的拓扑结构有哪些,各有什么优缺点?

第 2 章

# 计算机网络体系结构

## 2.1　网络体系结构

### 2.1.1　协议的定义和要素

计算机通信技术的飞速发展使计算机网络触及社会生活的方方面面，那么计算机网络怎样才能通信？计算机网络的本质是什么？要回答以上问题必须理解协议这个概念。

在计算机网络中，通信发生在不同系统的实体之间，实体(Entity)是能够发送和接收信息的任何事物。然而，两个实体间仅发送比特流就指望能相互理解是不可能的。要实现通信，实体之间必须遵循协议，协议是用来管理数据通信的一组规则。协议包括对数据格式、同步方式、传送速度、传送步骤、检纠错方式以及控制字符定义等问题做出统一规定，通信双方必须共同遵守。因此，也叫做通信控制规程，或称传输控制规程。

协议的核心要素是语法、语义和时序。

(1) 语法(Syntax)。语法规定通信双方"如何讲"，即指通信双方采用的数据格式、编码等，即规定数据与控制信息的结构和格式。例如，一个简单的协议可能将第一个 8 位数据作为发送者的地址，第二个 8 位数据作为接收者的地址，信息流的其余部分作为报文本身。

(2) 语义(Semantics)。语义规定了双方"讲什么"，指的是每一个比特片段的含义，通信双方在什么层次上定义通信，其内容是什么，也就是对发出的请求、执行的动作、对方的应答做出何种解释。如何解释一个特别的位模式，基于该解释应该采取什么操作？例如：SYN 表示同步，ACK 表示确认，NAK 表示否认等。

(3) 时序(Timing)。时序规定事件实现顺序的详细说明，即确定通信状态的变化和过程，指的是两个特性：报文发送的时间和发送的速率。例如，如果发送者以 100Mb/s 的速率发送而接收者只能以 1Mb/s 的速率处理数据，那么传输中会使接收者过载而造成数据的大量丢失。

语义表示要做什么，语法表示要怎么做，时序表示什么时候做。

### 2.1.2　协议的功能

**1. 分割与重组**

通信双方中的发送者发送出去的是报文，按照协议把报文分割成为信息包，这一过程叫

分割；接收方收到信息包后，把信息包重新组合成为报文，这一过程叫重组。

**2. 封装与拆装**

封装是指在发送的信息包的始端或者末端增加控制信息，其相反过程就叫拆装。

**3. 寻址**

网络中的设备如何才能相互识别，选择一条合适的路径。

**4. 排序**

排序是指对信息包的发送和接收顺序进行控制。

**5. 信息流的控制**

当网络中的信息流过大时协议所采用的一系列措施。

**6. 差错控制**

网络中传输的数据有可能会出现差错，当出现差错时，如何纠错，实现正确的传输。

**7. 同步**

网络中的通信双方需要高度的协同工作，双方需要知道何时开始发送数据，传输的速率是否一致，持续时间多长，发送时间间隔是多少等。为了避免发送方和接收方不能同步情况的出现，必须在发送端和接收端之间采取严格的同步措施。

**8. 连接的控制**

连接的控制是指通信双方建立和终止通信链路的过程。

## 2.1.3 层次和接口

计算机网络是一个结构复杂的系统，它的体系结构非常类似于现实世界中的邮件物流网络。为了更好地理解计算机网络体系结构，先来研究一下邮件物流网络。邮件物流网络由通信人活动、邮局服务业务、邮局转运业务、运输部门的运输业务等 4 个不同层次的网络组成，如图 2-1 所示。

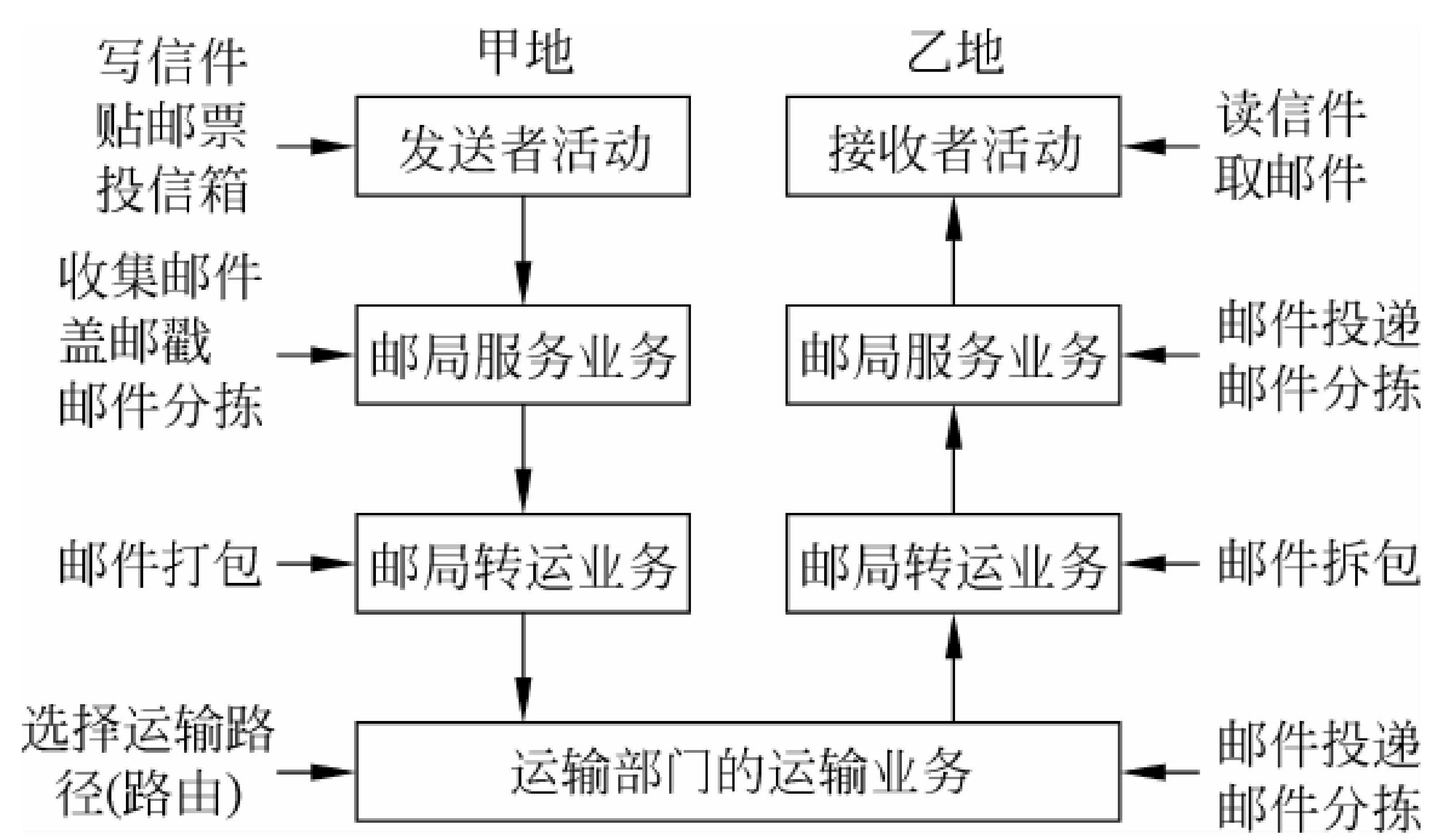



图 2-1 邮政物流系统中信件传递工作示意图

假如有一对好朋友，他们分住甲乙两地，甲要写信给乙。

甲地：

（1）写信人书写信件，按邮政系统的规定书写信封，贴上邮票，投入到邮箱中。

（2）邮递员到各处邮箱收集邮件，回到邮局盖上邮戳，进行分拣，装入邮包，按转运部门的要求贴上标签，送到转运部门。

（3）邮局转运部门把各个邮局送来的邮包分地区装入大邮包，按运输部门的要求贴上大邮包的标签，交给运输部门进行运送。

（4）运输部门按大邮包上所贴标签的地址，选择路径（空运、铁路、公路或者海运）进行运输。

乙地：

（1）运输部门收到不同地区送来的大邮包，分离出装有信件的邮包，转交到本地区的转运部门。

（2）转运部门拆开邮包，根据标签信息进行分拣，为各邮件选择合适的本地邮局。

（3）邮局拆开转运部门送来的邮包，根据信封上的信息，把信件交给管片邮递员，邮递员再把信件放到收件人的信箱中。

（4）收信人打开信箱，取回自己的信件，拆开阅读信件。

从以上的情况看，写信人的信件是按从上到下顺序流转的，每一层都是按照本层和下层联系的要求贴上标签，传到下一层位置。比如发信人把写好地址、贴好邮票的信件放入邮箱，邮箱是发信人和邮递员之间的一个联系点。发信人并不需要知道信件在邮局中是如何被分拣的，如何被打包的，如何被运输的等。发信人只管使用邮政系统的功能即可。

收信人的信件是按照从下往上顺序处理的。在每一层首先拆开邮包，根据标签上信息，再传递到上一层指定的位置，最后送到收件人的手里。同样，在收信端收信人只需要知道到信箱中取信就可以了，不需要知道信件是如何被转运，如何被分发，如何被投递。

邮件系统中，信件的格式、信封的大小及格式、邮包上面标签的格式等，这些都需要事先进行约定，在邮政系统的不同层次之间可以相互理解。我们把这种系统中通信的约定称为协议。

从总体上看，邮政系统庞大复杂，要研究管理比较困难，但把它要实现的功能分为 4 个层次后，每个层次功能相对较为独立简单，各层之间通过邮箱和标签进行联系。层次结构的提出，对复杂问题采用“分而治之”的方法，大大降低了解决复杂问题的难度。分层的思想涉及以下两个概念。

1）层次

当人们遇到非常复杂的事物的时候，总是把它划分为不同的层次，让不同的层次拥有不同的功能，分层可将庞大而复杂的问题转化为若干较小的局部问题，而较小的局部问题则较容易研究和解决。计算机网络体系结构是非常复杂的，人们也把它划分为不同的层次来描述它的结构和功能。功能是以层次划分为基础的，各层相对较为独立，上层是下层的用户，

下层是服务的提供者；上一层不需要知道下一层是如何实现的，仅知道通过层间的接口调用下层的服务；当任何一层发生变化时，只要接口未发生变化，其他层均不受影响。

2）接口

接口是各层间交换信息的连接点，邮件系统中邮箱和邮包上的标签都是接口，上一层通过接口调用下一层的服务，下一层通过接口向上一层提供服务。只要接口不变，即下层的功能不变，低层功能的具体实现方法不会影响其他层。

### 2.1.4　计算机网络体系结构的提出

和邮政系统一样，计算机网络系统也是非常庞大复杂的。要研究它，可以采用和邮政系统一样的策略，把它分为若干层，在层之间定义接口以及通信的协议。我们把计算机网络的层次结构模型和层间接口及通信的协议统称为计算机网络体系结构。

网络体系结构只是一个设计原则和抽象的概念，只涉及实现什么功能，而不涉及功能怎么实现的问题。采用网络体系结构来研究网络的优点是显而易见的，它简化了计算机网络的复杂程度，有利于计算机网络的开放和标准化。

## 2.2　ISO 与 OSI 参考模型

20 世纪 70 年代，许多著名的计算机公司纷纷推出自己的计算机网络体系结构。如 IBM 公司推出的系统网络体系结构（SNA），Digital 公司推出了数字网络体系结构（DNA），美国国防部推出了 TCP/IP 等。有了网络体系结构，在同一体系结构下的计算机就很容易连接到一起。但多种网络体系结构并存的结果是：选用了某家公司的网络体系结构，以后只有选用这家公司的产品，才能与以前的网络互联互通。

为了充分发挥计算机网络的作用，使不同计算机厂家的网络能够连接，相互通信，这时就需要一个国际标准，遵守国际标准的网络才能互联互通。国际标准化组织（ISO）成立了专门的委员会对网络体系结构进行研究，于 1981 年颁布了不基于具体机型、操作系统或公司的开放系统互连参考模型（OSI/RM），也就是七层网络通信模型，通常简称“七层模型”。

开放系统互连参考模型的分层思想使得复杂的网络体系结构变得层次分明，结构清晰，使整个网络的设计变成了对各层及层间接口的设计，因此容易设计和实现。网络中的每个节点都被划分为 7 个相同的层次结构；不同节点的相同层次拥有相同的功能；同一节点内各相邻层次间通过接口进行通信；每一个上级层次向下级层次提出服务请求，使用下层提供的服务；下层向上层提供服务；不同节点间对等层之间按对等层协议进行通信。

## 2.2.1　OSI 各层的功能

下面简要介绍 OSI 参考模型(图 2-2)每层协议的具体功能、处理的数据单元、地址信息及典型设备。

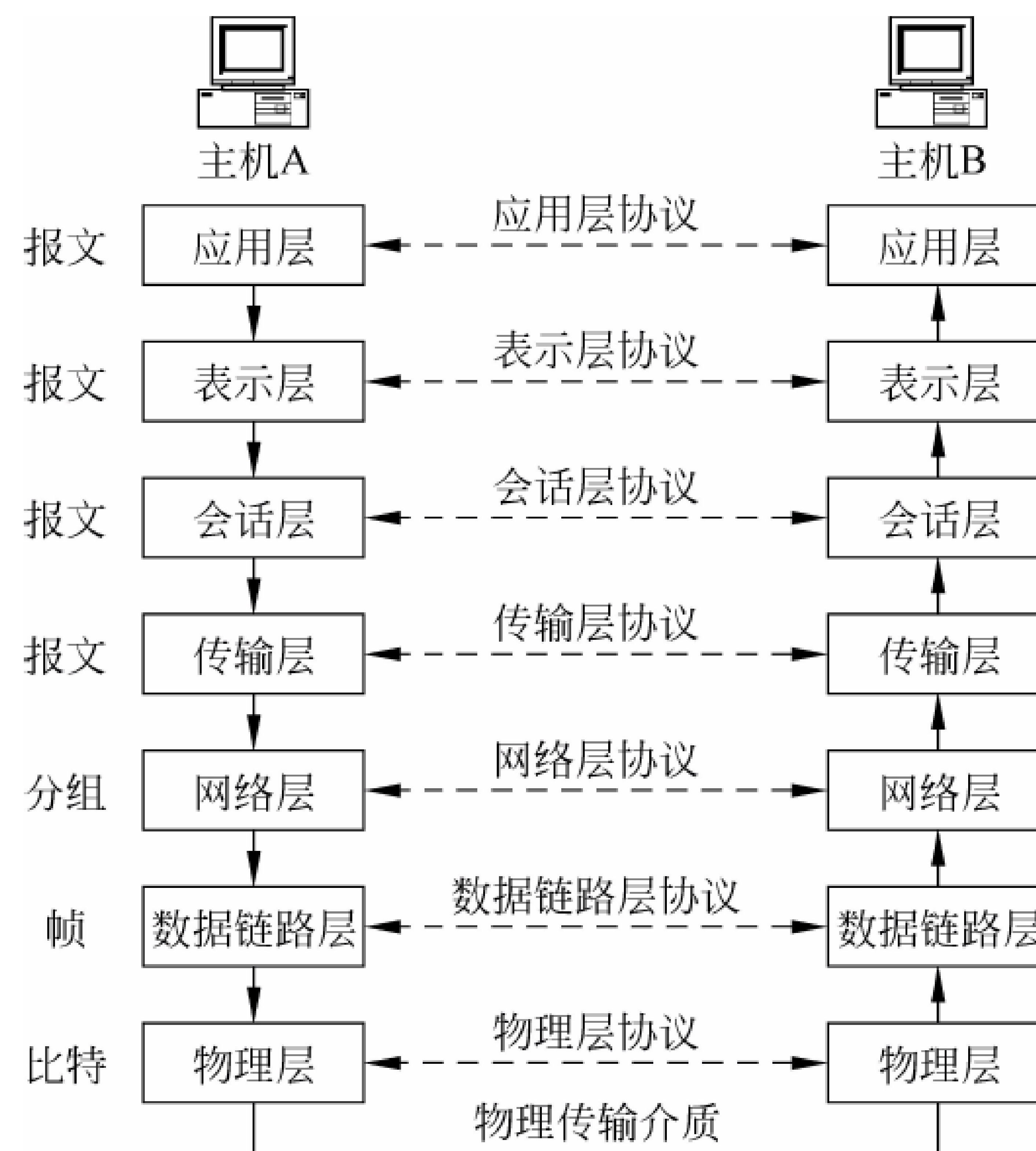



图 2-2　OSI/RM 网络模型的结构示意图

**1. 物理层**

物理层(Physical Layer)是 OSI 分层体系结构中的最底层,它建立在通信介质的基础上,实现系统和通信介质的物理连接,主要解决网络节点与物理信道如何连接的问题。它规定了激活、维持、关闭信道及通信端点之间的机械特性、电气特性、工程规范以及工作方式。虽然物理层不提供纠错服务,但它能够设定数据传输速率并监测数据出错率。

(1) 机械特性:详细说明了物理接口连接器的尺寸、引脚的数目、排列方式、电缆长度以及电缆所含导线的数目等。

(2) 电气特性:规定了在链路上传输二进制比特流的电气特性。比如:电压的高低、阻抗的匹配、传输速度与距离的限制等。

(3) 工程规范:规定各信号线的功能或作用。信号线按功能可分为数据线、控制线、时钟线和接地线等,工程规范要规定接口引脚的含义、特性、标准。

(4) 工作方式:规定接口间传输比特流的过程和顺序。如单工、半双工或全双工。

物理层需要解决的问题主要有信号衰减和噪声。因为介质吸收、反射或散射等原因造成不可避免的信号衰减,限制了信号的传输距离,因此,网络中经常采用中继器或集线器等

设备来对信号进行放大和整形。网络中也经常采用抵消、屏蔽、良好的端接和接地等措施来减少噪声,提高信噪比。

物理层的主要设备有中继器和集线器。

物理层的协议包括 EIA/TIA RS-232、EIA/TIA RS-449、V.35、RJ-45 等。

处理的数据是二进制比特信息。

处理的地址是直接面向物理端口的各个管脚。

**2. 数据链路层**

在物理层提供比特流服务的基础上,建立相邻节点之间的数据链路,通过差错控制提供数据帧(Frame)在信道上无差错的传输。

数据链路层(Data Link Layer)应具备如下功能:

(1) 链路连接的建立,拆除,分离。

(2) 帧定界和帧同步。链路层的数据传输单元是帧,协议不同,帧的长短和界面也有差别,但无论如何必须对帧进行定界。帧定界要解决的问题是接收方如何从接收到的比特流中准确地区分出一帧的开始和结束。常用的定界方法有字符计数法、带填充字符的首尾界符法、带填充位的首尾标志法和物理层编码违例法。

(3) 顺序控制,指对帧的收发顺序的控制。

(4) 差错检测和恢复。差错检测多用方阵码校验和循环码校验来检测信道上数据的误码,帧丢失等用序号检测;各种错误的恢复则常靠反馈重发技术来完成。

(5) 流量控制。数据链路层的流量控制主要采用等-停协议和滑动窗口协议。等-停协议的基本思想是发送方每发送一个数据帧,都要等待接收方的确认信息到来后,才发送下一帧,接收方每接收到一个数据帧后,都要向发送方发送一个确认帧,来确认正确接收到了数据帧。滑动窗口协议的基本原理是发送和接收方都会维护一个数据帧的序列,这个序列被称做窗口。发送方的窗口大小由接收方确定,目的在于控制发送速度,以免接收方的缓存不够大,而导致溢出,同时控制流量也可以避免网络拥塞。

数据链路层的主要设备有二层交换机和网桥。

数据链路层协议的代表包括 SDLC、HDLC、PPP、STP、帧中继等。

数据链路层处理的数据单元是数据帧。

处理的地址是硬件的物理地址,如网卡的 MAC 地址。

**3. 网络层**

计算机网络中两台计算机之间进行通信时可能会经过很多个数据链路,也可能还要经过很多通信子网。网络层(Network Layer)的任务就是选择合适的网间路由和交换节点,确保数据及时传送。网络层将数据链路层提供的帧组成数据包,包中封装有网络层包头,其中含有逻辑地址信息——源站点和目的站点的网络地址。网络层还可以实现拥塞控制、网际互连等功能。IP、路由协议和地址解析协议(Address Resolution Protocol,ARP)都是在网络层上的。

网络层的主要功能是：

（1）路由选择和中继。根据一定的原则和路由选择算法在多节点的通信子网中选择一条最佳路径。

（2）激活、终止网络连接。

（3）在一条数据链路上复用多条网络连接，多采取分时复用技术。

（4）差错检测与恢复。

（5）排序、流量控制。

（6）服务选择。

网络层的主要设备是路由器，三层交换机。

网络层的协议有 IP、IPX、RIP、OSPF 等。

网络层处理的数据单元是数据包。

网络层处理的地址是逻辑地址，如计算机或路由器的端口地址 192.168.1.11。

**4. 传输层**

传输层（Transport Layer）的主要功能是：负责两个进程之间的通信，为上层提供端到端（最终用户到最终用户）的、透明的、可靠的数据传输服务。所谓透明的传输是指在通信过程中传输层对上层屏蔽了通信传输系统的具体细节。

传输层的功能：

（1）分割与重组数据。在发送方，传输层将会话层送来的数据分割成较小的数据单元，并在这些数据单元的头部加上一些相关控制信息形成段或报文，报文的头部包含源端口号和目标端口号。在接收方，数据经通信子网到达传输层后，将各报文原来在发送方加上的报文头等控制信息去掉，然后按照正确的顺序进行重组，送给会话层。

（2）按端口号寻址。传输层通过端口号寻找端点上的进程，使不同端口上的进程进行相互通信。

处理的协议是 TCP、UDP、SPX 等。

传输层的数据单元是报文段。

处理的地址是进程标识，如 TCP 和 UDP 端口号。

**5. 会话层**

会话层（Session Layer）也称为会晤层或对话层，会话层不参与具体的传输，它提供包括访问验证和会话管理在内的建立和维护应用之间通信的机制。如服务器验证用户登录便是由会话层完成的。

会话层提供的服务可使应用建立和维持会话，并能使会话获得同步。会话层使用校验点可使通信会话在通信失效时从校验点继续恢复通信。这种能力对于传送大的文件极为重要。会话层、表示层、应用层构成开放系统的高 3 层，面对应用进程提供分布处理，对话管理，信息表示，恢复最后的差错等。

处理的数据单元是报文。

**6. 表示层**

表示层(Presentation Layer)主要负责用户信息的语法表示问题,它将欲交换的信息从适合于某一用户的抽象语法转换成适合于 OSI 系统内部的传递语法。即提供格式化的表示和数据转换服务。数据的压缩与解压、加密与解密、数据格式的转换等都是在表示层完成的。

处理的数据单元是报文。

**7. 应用层**

应用层(Application Layer)是 OSI 中的最高层,也是最接近用户的层。这一层是操作系统或网络应用程序为用户提供网络服务的接口。

处理的协议有 FTP、Telnet、HTTP、SNMP 等。

处理的数据单元是报文。

处理的地址是进程标识,即端口号,如 HTTP 协议使用的端口号是 80。

OSI 是一个理想的模型,一般的系统只涉及其中的几层,很少有系统能够包含完整的七层。它是一个定义得很好的协议规范集,它是一个理论的指导性模型,是一个理想的模型。要理解 OSI 模型要从以下几个概念来理解。

(1) OSI 模型的核心思想是把系统分层,不同层解决不同的问题。

第 1 层和第 2 层,即物理层和数据链路层解决网络信道问题。

第 3 层和第 4 层,即网络层和传输层解决传输问题。

第 5、6、7 层,即会话层、表示层和应用层解决应用进程之间的访问问题。

(2) “透明”在 OSI 中是一个很重要的概念。它表示某一个实际存在的事物好像不存在一样。例如计算机网络中存在着大量的物理设备,物理层对于数据链路层来说,就是要尽可能地屏蔽掉各种设备和介质的具体特征,使得数据链路层感觉不到物理层各种设备和介质的差别,数据链路层只是调用物理层传输比特流的功能。

(3) OSI 模型从控制上分为两部分。

第 1~3 层:即物理层、数据链路层和网络层属于通信子网,负责数据的传输,转发、交换等通信方面的问题。

第 4~7 层:即传输层、会话层、表示层和应用层属于资源子网,负责数据的处理、网络服务、网络资源的访问和服务方面的问题。

## 2.2.2 OSI 参考模型节点间的数据流

OSI 参考模型节点间的数据流如图 2-3 所示。

在 OSI 模型中,数据是如何在主机之间传递的,是理解网络中主机之间通信的关键。OSI 的七层运用各种各样的控制信息来和其他计算机系统的对应层进行通信。这些控制信息包含特殊的请求和说明,它们在对应的 OSI 层间进行交换。每一层数据的头和尾是两个携带控制信息的基本形式。对于从上一层传送下来的数据,附加在前面的控制信息称为头,

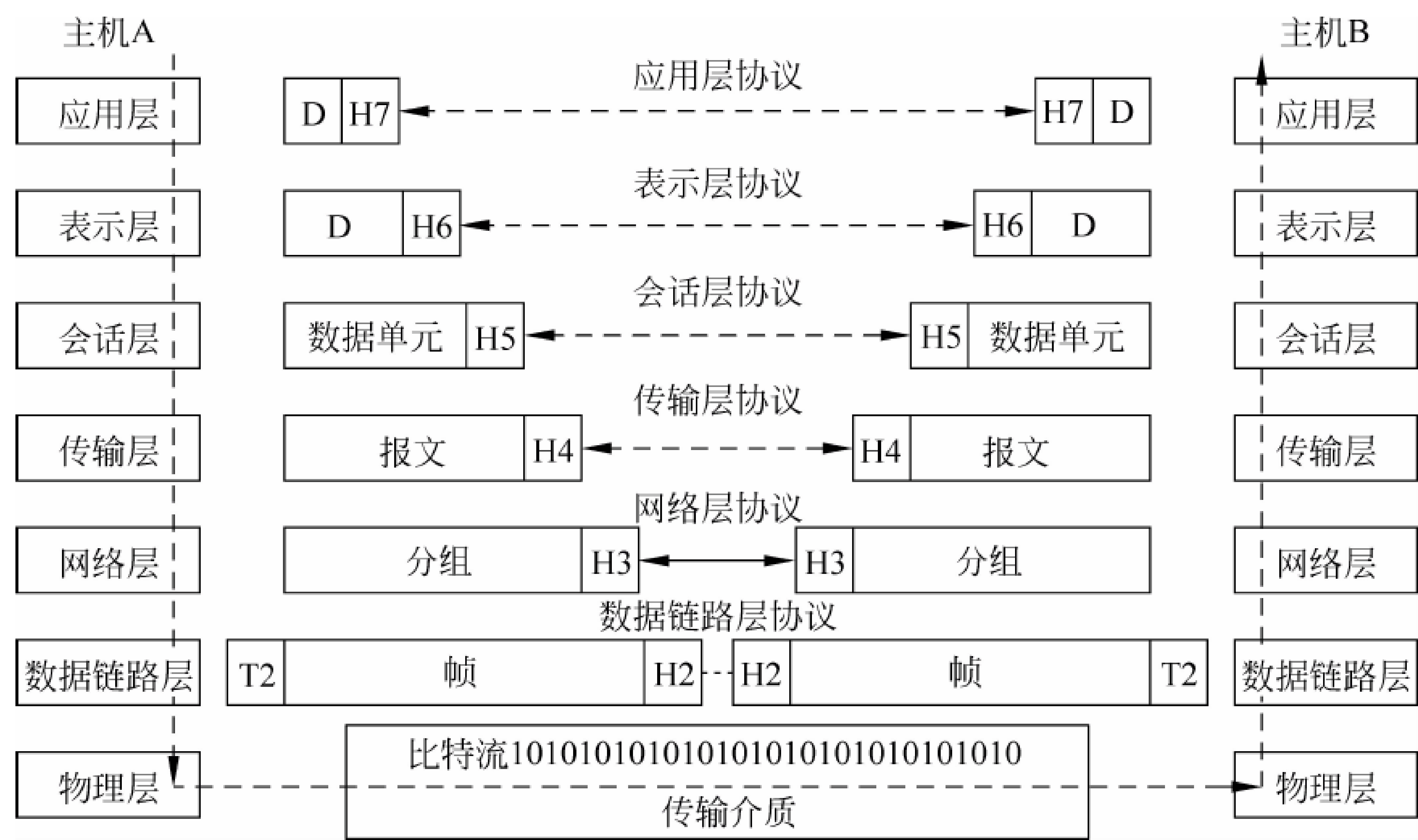



图 2-3　OSI 节点间的数据流

附加在后面的控制信息称为尾。然而，在来自上一层的数据增加协议头和协议尾，对一个 OSI 层来说并不是必需的。下面来看一下数据流在 OSI 模型中的流动情况。

（1）当主机 A 中的应用进程 A 的数据传送到应用层时，应用层为数据加上本层控制报头 H7 后，组织成应用层的数据服务单元，然后再传输到表示层。

（2）表示层接收到这个数据单元后，并不知道接收到的数据哪些是应用层的原始数据，哪些是控制信息 H7，只能把它们作为一个整体来对待，再加上本层的控制报头 H6，组成表示层的数据服务单元，传送到会话层。以此类推，数据传送到传输层。

（3）传输层接收到这个数据单元后，加上本层的控制报头 H4，就构成了传输层的数据服务单元，它被称为报文（Message）。

（4）传输层的报文传送到网络层时，由于网络层数据单元的长度有限制，传输层报文将被分成多个较短的数据字段，加上网络层的控制报头 H3，就构成网络层的数据服务单元，它被称为分组（Packet）。

（5）网络层的分组传送到数据链路层时，加上数据链路层的控制信息 H2，再加上一个尾信息 T2，就构成了数据链路层的数据服务单元，它被称为帧（Frame）。

（6）数据链路层的帧传送到物理层后，物理层将以比特流的方式通过传输介质传输出去。当比特流到达目的节点计算机 B 时，再从物理层依层上传，每层将各自的控制信息头去掉，再将用户数据上交高层，最终将进程 A 的数据送给计算机 B 的进程 B。

从上面的过程可以看出：数据从主机 A 的应用进程 A 发出，每一层都会加上控制信息，即有一个封装过程；在主机 B 中每一层又依次发挥作用，将各自的控制信息去掉，即拆封。尽管应用进程 A 的数据在 OSI 环境中经过复杂的处理过程，才能送到另一台计算机的

应用进程 B,但对于每台计算机的应用进程来说,OSI 环境中数据流的复杂处理过程是透明的。应用进程 A 的数据好像是“直接”传送给应用进程 B,这就是开放系统在网络通信过程中最本质的作用。

## 2.3 TCP/IP 参考模型

尽管 OSI 参考模型得到了全世界的认同,但是因特网历史上和技术上的开发标准都是 TCP/IP 模型(Transmission Control Protocol/Internet Protocol,传输控制协议/网际协议)。

TCP/IP 起源于 20 世纪 60 年代末美国政府资助的一个网络分组交换研究项目,TCP/IP 是发展至今最成功的通信协议,它被用于当今所构筑的最大的开放式网络系统 Internet 之上。

TCP 和 IP 是两个独立且紧密结合的协议,负责管理和引导数据报文在 Internet 上的传输。二者使用专门的报文头定义每个报文的内容。TCP 负责和远程主机的连接,IP 负责寻址,使报文被送到其该去的地方。TCP/IP 也分为不同的层次,每一层负责不同的通信功能。但 TCP/IP 简化了层次设备(只有 4 层),由下而上分别为网络接口层、网际层、传输层、应用层。

表 2-1 是 OSI 模型与 TCP/IP 模型之间的对应关系。

**表 2-1 OSI 模型和 TCP/IP 模型的对应关系**

| OSI 参考模型 | TCP/IP 模型 |
|---|---|
| 应用层 | 应用层 |
| 表示层 | |
| 会话层 | |
| 传输层 | 传输层 |
| 网络层 | 网际层 |
| 数据链路层 | 网络接口层 |
| 物理层 | |

由于 TCP/IP 是 OSI 模型之前的产物,所以两者间不存在严格的层对应关系。在 TCP/IP 模型中并不存在与 OSI 中的物理层与数据链路层相对应的部分,相反,由于 TCP/IP 的主要目标是致力于异构网络的互连,所以同 OSI 中的物理层与数据链路层相对应的部分没有进行任何限定。

表 2-2 是 TCP/IP 各层的描述。

**表 2-2 TCP/IP 各层的描述**

| 层 | 描　述 | 协　议 |
|---|---|---|
| 应用层 | 定义了 TCP/IP 应用协议及主机程序与要使用网络的传输层服务之间的接口 | HTTP、Telnet、FTP、TFTP、SNMP、DNS、SMTP、X-Windows 以及其他应用协议 |
| 传输层 | 提供端到端的可靠或不可靠的传输服务,可以实现流量控制和负载均衡 | TCP、UDP |

续表

| 层 | 描　　述 | 协　　议 |
| --- | --- | --- |
| 网际层 | 将数据装入 IP 数据报，包括用于在主机间及经过网络转发数据报时所用的源和目标的地址信息。实现 IP 数据报的路由 | IP、ICMP、ARP、RARP |
| 网络接口层 | 负责数据的分帧与拆封，使用 MAC 地址访问传输介质，进行错误检测与修正 | 以太网、令牌环、FDDI、X. 25、帧中继、RS-232、v. 35 |

### 1. 应用层

TCP/IP 协议的最高层是应用层，它对应 OSI 模型的上三层，即应用层、表示层、会话层。它向用户提供调用和访问网络中各种应用程序的接口，并向用户提供标准的应用程序及相应的协议。应用层的协议主要有：

(1) 超文本传输协议(Hypertext Transfer Protocol，HTTP)，默认使用 80 端口，或使用 8080 端口，用于提供 WWW 服务，实现了 Web 服务器和用户之间的超文本数据的传输。

(2) 远程终端协议(Telnet)，它默认使用 23 端口，用于实现在因特网的远程登录功能，即一台网络主机上的用户使用该项服务登录到另一台主机，并在远程主机上进行工作，用户的主机就好像远程主机的一个终端。

(3) 文件传输协议(File Transfer Protocol，FTP)，默认使用 20/21 端口，用于实现文件的交互式传输，它允许把文件上传到 FTP 服务器上，也可以从 FTP 服务器上下载文件。

(4) 简单网络管理协议(Simple Network Management Protocol，SNMP)使用默认的 161 端口，实现管理和监控网络设备。

(5) 域名系统(Domain Name System，DNS)，或称域名服务(Domain Name Service，DNS)。域名是由圆点分开的一串单词或缩写组成的，每一个域名都对应一个唯一的 IP 地址。域名系统把不便于记忆的 IP 地址转换为便于记忆的域名，方便人们上网。

(6) 简单邮件传输协议(Simple Mail Transfer Protocol，SMTP)，默认使用 25 端口，它负责电子邮件的传递，用户发送电子邮件时，先使用 SMTP 协议把邮件传到本地的 SMTP 服务器上，该服务器再把邮件传到对方的邮件服务器上。

(7) 邮局协议(Post Office Protocol 3，POP3)即邮局协议的第 3 个版本，它使用 TCP 的 110 端口，它是规定个人计算机如何连接到互联网上的邮件服务器，接收邮件的协议。

### 2. 传输层

传输层又称运输层，它提供端到端的通信服务，它对应于 OSI 模型中的传输层，传输层包括两个主要的协议。

传输控制协议(Transmission Control Protocol，TCP)是一种面向连接的高可靠的传输层协议，它提供了流量控制和拥塞控制。它传输的数据单位是报文。

用户数据报协议(User Datagram Protocol，UDP)是一种面向无连接的，不可靠的协议，它也提供了流量控制和拥塞控制，但它传输的数据单位是分组。

### 3. 网际层

网际层又称为互联层，它对应于 OSI 模型中的网络层，因为该层中主要使用 IP 协议，所以也称为 IP 层。网际层主要提供相邻节点之间数据分组的寻址和路由服务。它包括以下协议。

（1）网络协议（Internet Protocol，IP）主要负责为数据包提供寻址和路由服务。

（2）网际控制报文协议（Internet Control Message Protocol，ICMP），它用于在 IP 主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。

（3）地址解析协议（ARP）主要用于将主机的 IP 地址转换为物理地址（MAC 地址）。

（4）逆向地址解析协议（Reverse Address Resolution Protocol，RARP）用来完成物理地址到 IP 地址的转换。

### 4. 网络接口层

网络接口层对应于 OSI 模型中的数据链路层和物理层，是 TCP/IP 的最底层。主要负责向网络媒体发送 TCP/IP 数据包并从网络媒体接收 TCP/IP 数据包。TCP/IP 独立于网络访问方法、帧格式和媒体，可以使用 TCP/IP 接口层技术组织以太网、无线局域网和广域网网络之间进行通信。

TCP/IP 支持的网络接口类型主要有：标准以太网、令牌环、FDDI、ATM、点对点协议（Point to Point Protocol，PPP）等。

## 2.4 OSI 与 TCP/IP 体系结构的比较

OSI 模型即开放式系统互联模型是一个参考标准，解释协议相互之间应该如何相互作用。TCP/IP 协议是美国国防部发明的，是让互联网成为了目前这个样子的标准之一。开放式系统互联模型中没有清楚地描绘 TCP/IP 协议，但是在解释 TCP/IP 协议时很容易想到开放式系统互联模型。

### 1. OSI 与 TCP/IP 的共同之处

（1）都采用了层次结构，这样将复杂的问题简单化，易于处理。但无论是 OSI 参考模型还是 TCP/IP 体系结构都不是完美的，对二者的评论与批评都很多。

（2）各层功能大体上相同，都有网络层、传输层和应用层。两者都解决了异构网络的互连问题。在两个模型中，传输层及以上的各层都是为通信的进程提供点到点、与网络无关的传输服务。

（3）两者都以协议栈的概念为基础，并且协议栈中的协议相互独立。

**2. OSI 与 TCP/IP 的区别**

(1) OSI 与 TCP/IP 虽然都分层，但各层定义却不尽相同。OSI 模型分为 7 层，而 TCP/IP 只有 4 层，除网络层、传输层和应用层外，其他各层都不相同。TCP/IP 虽然也分层但各层之间的调用关系不像 OSI 模型那么严格。

(2) OSI 作为国际标准是由多个国家共同努力制定的，为了照顾各个国家的利益，造成标准大而全，难以实现。而 TCP/IP 并不是作为国际标准开发的，它只是对一种已有标准的概念性描述。因为它简单高效，可操作性强，因此，TCP/IP 已经成为事实上的国际标准。

(3) TCP/IP 一开始就对面向连接服务和无连接服务并重，而 OSI 在开始时只强调面向连接这一种服务。

(4) TCP/IP 较早就有较好的网络管理功能，而 OSI 到后来才开始考虑这个问题。

# 思考与练习

**一、填空题**

1. 从高到低 OSI 参考模型依次是________、________、________、________、________、________和________。

2. 网络的参考模型有两种：________和________

3. 网络协议的三要素：________、________和________。

4. 具有路由功能的交换机被称为________。

5. 中继器工作在 OSI 参考模型的________上，其功能是对衰减的信号进行再生和放大。

6. 万维网(WWW)服务的传输协议是________。

**二、选择题**

1. 下列哪一个是传输层的协议？(　　)

A. LLC　　B. IP　　C. SQL　　D. UDP

2. 下列哪些是表示层的例子？(　　)

A. MPEG　　B. JPEG　　C. ASCII　　D. TFTP

3. 将发送方数据转换成接收方的数据格式是由 OSI 参考模型的(　　)层实现的。

A. 应用层　　B. 表示层　　C. 会话层　　D. 传输层

4. 请说出在 OSI 模型数据封装过程中，自顶向下的协议数据单元(PDU)名字：(　　)。

A. 数据流、数据段、数据帧、数据包、比特

B. 数据流、数据段、数据包、数据帧、比特

C. 数据帧、数据流、数据段、数据包、比特

D. 比特、数据帧、数据包、数据段、数据流

5. OSI 模型下列不属于表示层功能的有(　　)。

A. 加密　　B. 压缩　　C. 格式转换　　D. 区分服务

6. 数据到达网络层以后在 OSI 模型里我们称之为(　　)。

A. 数据段　　B. 数据包　　C. 数据帧　　D. 数据位(BIT 流)

7. FTP 是文件传输协议,它使用的端口是(　　)。

A. 21 22　　B. 80　　C. 25　　D. 20 21

8. TCP/IP 的网络层含有四个重要的协议,分别为(　　)。

A. IP,ICMP,ARP,UDP　　B. TCP,ICMP,UDP,ARP

C. UDP,IP,ICMP,RARP　　D. IP,ICMP,ARP,RARP

9. 下列哪个不是数据链路层的网络连接设备?(　　)

A. 网卡　　B. 路由器　　C. 交换机　　D. 网桥

10. 在计算机网络体系结构中,要采用分层结构的理由是(　　)。

A. 可以简化计算机网络的实现

B. 各层功能相对独立,各层因技术进步而做的改动不会影响到其他层,从而保持体系结构的稳定性

C. 比模块结构好

D. 只允许每层和其上、下相邻层发生联系

11. 建立计算机网络的目的在于(　　)。

A. 资源共享　　B. 建立通信系统

C. 建立自动办公系统　　D. 建立可靠的管理信息系统

12. TCP/IP 参考模型中,应用层协议常用的有(　　)。

A. Telnet,FTP,SMTP 和 HTTP

B. Telnet,FTP,SMTP 和 TCP

C. IP,FTP,SMTP 和 HTTP

D. IP,FTP,DNS 和 HTTP

13. 文件传输是使用下面的(　　)协议。

A. SMTP　　B. FTP　　C. UDP　　D. Telnet

14. 网络中实现远程登录的协议是(　　)。

A. HTTP　　B. FTP　　C. POP3　　D. Telnet

15. 在计算机网络的 ISO/OSI 七层模型中,负责选择合适的路由,使发送的分组能够正确无误地按照地址找到目的站并交付给目的站的是(　　)。

A. 网络层　　B. 数据链路层

C. 运输层　　D. 物理层

16. 数据传输中的“噪声”指的是(　　)。
   A. 信号在传输过程中受到的干扰　　B. 传输过程中信号的衰减
   C. 音频信号在传输过程中的失真　　D. 以上都是

**三、问答题**

1. 试画出 OSI 参考模型的层次结构,并简述各层的基本功能。
2. 描述 TCP/IP 模型。
3. 比较 OSI 模型和 TCP/IP 模型的区别与联系。

第3章

# 数据通信基础

计算机网络是计算机和通信技术发展的产物，网络技术的发展离不开通信技术。了解并掌握数据通信基础知识对理解网络工作原理、把握网络组建和管理方法很有帮助。本章将介绍基本的数据通信知识，使读者对网络通信中的常见术语和技术有基本的认识和把握。

## 3.1　数据通信的基本概念

### 3.1.1　数据通信系统的组成

计算机网络中，数据通信系统的任务是把源计算机所产生的数据迅速、可靠、准确地传输到目的计算机或专用外设。数据通信系统由信源、信道和信宿组成。数据通信系统的组成如图3-1所示。



图3-1　数据通信系统的组成(1)

信源即信息的来源，是数据的发送方；信宿即信息的目的地，是数据的接收方；信道即传输数据的通道。信源产生的数据经过编码后以信号的形式在信道上传输，并在信宿端解码为数据。

通信系统中的信源和信宿称为数据终端设备(Data Terminal Equipment，DTE)，一般网络中常用的DTE设备有计算机、路由器、网络打印机等。大多数时候，DTE是不能直接与信道相连的，需要一种称为数据通信设备(Data Communications Equipment，DCE)的设备完成通信管理和信号转换等工作。因而，数据通信系统的组成也可表示为图3-2。



图3-2　数据通信系统的组成(2)

通信系统中 DCE 还有一个重要的作用就是控制通信频率(时钟)。因而,一对 DTE 与 DCE 的通信中,总是由 DCE 提供时钟信号,DTE 则依靠 DCE 提供的时钟工作。常用的 DCE 有调制解调器(Modem)、CSU/DSU、交换机等。

在信源和信宿之间建立起的有效传输数据的物理通道称为信道,能容纳各种物理信号。不同的信道容纳信号的能力是不同的,如电话线路等模拟通信信道、专用数字通信信道、宽带电缆(Community Antenna Television,CATV)和光纤等。

### 3.1.2　信息、数据和信号

数据通信系统中,信息、数据和信号含义不同而又相互关联。信息是指数据的内容和解释,它反映了客观事物的存在形式或运动状态。

数据是信息的载体,是信息的表现形式。数据可分为模拟数据和数字数据两大类。模拟数据是在某个区间内连续变化的值,例如声音和视频都是幅度连续变化的波形,又如温度和压力也都是连续变化的值;数字数据是离散的值,例如文本信息、整数、计算机能够处理的二进制数 0 和 1。

信号则是数据的电子或电磁编码,是数据在传输过程的具体物理表现形式。对应于模拟数据和数字数据,信号也可分为模拟信号和数字信号。模拟信号是随时间连续变化的电流、电压或电磁波,可以利用其某个参量(如幅度、频率或相位等)来表示要传输的数据;数字信号则是一系列离散的电脉冲,可以利用其某一瞬间的状态来表示要传输的数据,如方波 ⎍⎍ 。

### 3.1.3　基带、频带与宽带

通信系统中信号每秒钟变化的次数叫频率,用赫兹(Hz)作单位。信号的频率有高有低就像声音有高有低一样,低频到高频的范围叫频带(频率带宽),不同的信号有不同的频率带宽,有的适合在信道上直接传输,大部分则不适合在信道上直接传输,需经过转换。

**1. 基带**

信源发出的没有经过调制的原始电信号所固有的频带称为基本频带,简称基带。其特点是频率较低,信号频谱从零频附近开始。基带信号可分为数字基带信号和模拟基带信号,如说话的声波就是模拟基带信号;而计算机中二进制数的电子编码方波则是数字基带信号。

**2. 频带与宽带**

频带是指对基带信号调制后所占用的高频率带宽。在通信中,由于基带信号具有频率很低的频谱分量,出于抗干扰和提高传输率考虑一般不宜直接传输,需要把基带信号变换成其频带适合在信道中传输的信号,变换后的信号就是频带信号。

宽带是指比音频更宽的频率范围,包括大部分电磁波频谱。采用频分多路复用的形式可以把一个宽带物理信道分成多个子信道,每个子信道传输一路频带信号,从而实现高速传

输。如 CATV、ISDN 等。

### 3.1.4 数据通信技术指标

数据通信的任务是传输数据信息，希望达到传输速度快、出错率低、信息量大、可靠性高，并且既经济又便于使用和维护。这些要求可以使用下列技术指标加以描述。

**1. 数据传输率**

数据传输率是指单位时间内信道上所能传输的数据量。可用“比特率”和“波特率”来表示。

数据传输速率在数值上，等于每秒钟传输构成数据代码的二进制比特数，单位为比特/秒，记做 b/s。常用的数据传输速率单位有：Kb/s、Mb/s、Gb/s 与 Tb/s，目前最快的以太局域网理论传输速率为 10Gb/s。

数据传输速率计算公式：$S=1/T(\log_2 N)$。

其中 $T$ 为一个数字脉冲信号的宽度或重复周期，单位为秒；$N$ 表示一个脉冲所能表示的有效值状态，通常 $N=2^K$（$K$ 为二进制信息的位数）。当 $N=2$ 时，数据传输速率公式简化为：$S=1/T$，表示数据传输率等于码元脉冲的重复频率。

“波特率”也称“码元速率”、“调制速率”或者“信号传输速率”，是指每秒传输的码元数，单位为波特，记做 Baud。若每个码元所含的信息量为 1 比特，则波特率等于比特率。计算公式：$B=1/T(\text{Baud})$，式中 $T$ 为信号码元的宽度，单位为秒。

由以上两公式可以得出：$S=B\log_2 N(\text{b/s})$，或 $B=S/\log_2 N(\text{Baud})$。

在计算机中，一个符号的含义为高低电平，分别代表逻辑“1”和逻辑“0”，所以每个符号所含的信息量刚好为 1 比特，因此在计算机通信中，常将“比特率”称为“波特率”。

**2. 信道带宽**

信道带宽（Bandwidth）是指信道每秒传输的最大字节数，也就是一个信道的最大数据传输速率，单位也是“位/秒”。高带宽意味着系统的高处理能力。带宽与数据传输速率是有区别的，前者表示信道的最大数据传输速率，是信道传输数据能力的极限，而后者是实际的数据传输速率。像公路上的最大限速与汽车实际速度的关系一样。

带宽本来是指某个信号具有的频带宽度，其单位是赫兹（或千赫兹，兆赫兹），过去的通信主干线路都是用来传送模拟信号，带宽表示线路允许通过的信号频带范围。但是，当通信线路用来传送数字信号时，传送数字信号的速率即数据传输率成为数字信道的最重要指标，习惯上仍延续使用“带宽”来作为“数据传输率”的同义语。

**3. 信道容量**

信道的传输能力是有一定限制的，信道的数据传输速率的上限，称为信道容量，一般表示单位时间内最多可传输的二进制数据的位数。信道容量与信道带宽、噪声功率和信号功率的关系为：$C=W\log_2(1+S/N)$。

$C$ 为信道容量；$W$ 为信道带宽；$N$ 为噪声功率；$S$ 为信号功率。

**4. 误码率**

误码率($P_e$)是指二进制数据位传输时出错的概率。它是衡量数据通信系统在正常工作情况下的传输可靠性的指标。在计算机网络中,一般要求误码率低于 $10^{-6}$,若误码率达不到这个指标,可通过差错控制方法检错和纠错。

误码率计算公式为:$P_e = N_e / N$。式中的 $N_e$ 为其中出错的位数,$N$ 为传输的数据总位数。

**5. 信道延迟**

信号沿信道传输需要一定的时间,即信道延迟。信道延迟=计算机的发送和接收处理时间+传输介质的延迟时间+发送设备和接收设备的响应时间+通信设备的转发和等待时间。信道延迟越小,则通信系统的性能越高。

### 3.1.5　多路复用

数据通信系统中,信道的带宽或容量往往超过传输单一信号的需求。为了有效地利用通信线路,可以使用多路复用技术(Multiplexing)将多个数据流在一条物理链路上传输。常见的多路复用技术包括频分多路复用 FDM、时分多路复用 TDM、波分多路复用 WDM、码分多路复用 CDM。

远距离传输系统中使用多路复用技术可大大节省电缆的安装和维护费用。

**1. 频分多路复用**

频分多路复用(Frequency-Division Multiplexing,FDM),是指物理信道的载波带宽被划分为多种不同频带的子信道,每个子信道可以并行传送一路信号,如图 3-3 所示。

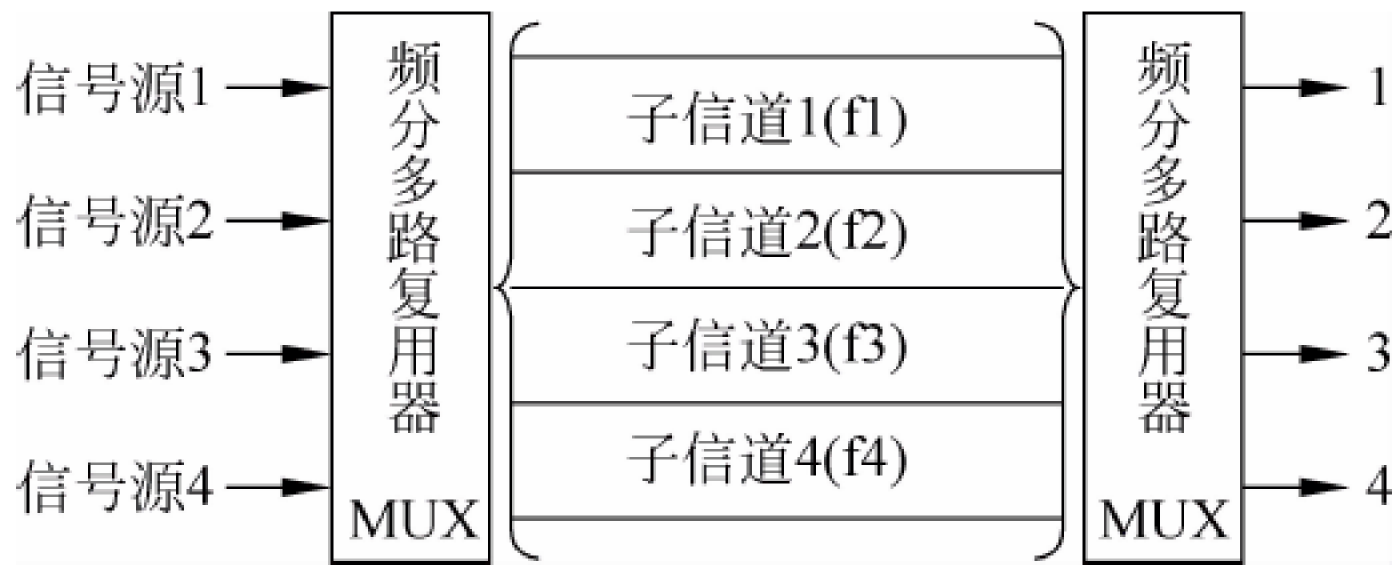



图 3-3　频分多路复用示意图

FDM 比较适合于传输模拟信号,常用于模拟传输的宽带网络中。宽带网络中信道的可用频带被分成若干个互不交叠的频段,每路信号用其中一个频段传输,再用频分多路复用器将信道上的多路信号分离,送给不同的信宿接收。

**2. 时分多路复用**

时分多路复用(Time-Division Multiplexing,TDM),是将物理信道的传输时间分为许多时间片(又称为时隙),而将若干个时隙组成时分复用帧,用帧中某一固定序号的时隙组成一个子信道,每个子信道传输一路信号。

时分多路复用又分为同步时分(Synchronous TDM,STDM)和异步时分(Asysnchronous

TDM,ATDM)。同步时分指多个发送端以固定的时隙分配信道,如图 3-4 所示;异步时分又称统计时分复用,它能动态地按需分配时隙:只给想发送数据的发送端分配其时隙段,当用户暂停发送数据时,则不给它分配时隙,以避免每个时隙段中出现空闲时隙。TDM 技术广泛应用于包括计算机网络在内的数字通信系统。

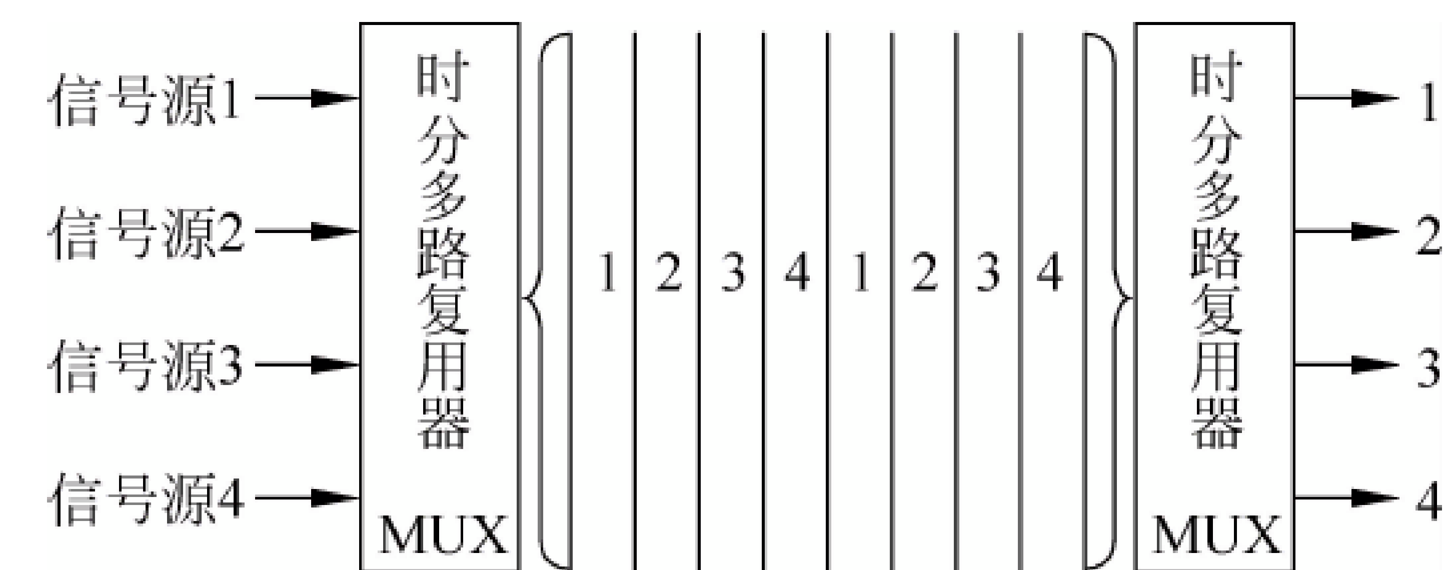



图 3-4　同步时分多路复用示意图

**3. 波分多路复用**

波分多路复用(Wave-Division Multiplexing,WDM),是在同一根光纤中同时传输两个或众多不同波长光信号的技术。WDM 将多个不同波长的光信号在发送端经合波器(Multiplexer)汇合在一起,并耦合到同一根光纤中进行传输,在接收端,经分波器(Demultiplexer)将各种波长的光载波信号分离,然后由光接收机作进一步处理以恢复原始信号。WDM 极大地提高了光纤的传输容量,是当前光纤通信网络扩容的主要手段。

**4. 码分多路复用**

码分多路复用(Code-Division Multiplexing,CDM),又称码分多址。我们常说的 CDMA 就是码分多路复用接入。每个用户可在同一时间使用同样的频带进行通信,但使用的是基于码型的分割信道的方法,即为每个用户分配一个地址码,各个码型互不重叠,通信各方之间不会相互干扰。码分多路复用主要用于无线通信系统,特别是移动通信系统。它不仅可以提高通信的话音质量和数据传输的可靠性以及减少干扰对通信的影响,而且增大了通信系统的容量。

## 3.2　数据传输方式

数据传输方式是指数据在信道上传递的方式。按被传输的数据信号的特点,可分为基带传输、频带传输和宽带传输;按数据传输的顺序可分为并行传输和串行传输;按数据传输的流向和时间可分为单工、半双工和全双工传输;按数据传输的同步方式可分为同步传输和异步传输。

### 3.2.1　基带传输、频带传输与宽带传输

**1. 基带传输**

基带传输是指在信道中直接传送基带信号,传输介质的整个信道被一个基带信号占用。

基带传输不需要调制解调器，设备花费小，具有速率高和误码率低等优点；但是，数字基带直接传送数字，传输的速率愈高，传输的距离愈短。因此，基带传输比较适合短距离传输，如音频市话、计算机和外设间的传输、大多数局域网的信号传输。常见的网络设计标准10Base-T 使用的就是基带传输。

**2. 频带传输**

频带传输是先将基带信号变换（调制）成便于在模拟信道中传输的、具有较高频率范围的频带信号，再将这种频带信号在模拟信道中传输。计算机网络的远距离通信通常采用的是频带传输。

频带传输能克服基带传输同频带过宽的缺点，提高线路的利用率；但是需要在发送端和接收端增加信号频率变换设备（调制解调器），费用相应增加。家庭用户拨号上网就属于这一类通信。

**3. 宽带传输**

宽带传输是指利用频分多路复用技术，将信道容量分解成两个或更多的信道，每个信道可以携带不同的信号，所有信道都可以同时发送信号，这就是宽带传输。宽带传输数据传输速率范围为 0～400Mb/s，而通常使用的传输速率是 5～10Mb/s。宽带传输优点是多路复用，信道容量大大增加；相比基带传输，宽带传输距离较远，可达几十千米。网络通信中广泛采用宽带传输技术。

## 3.2.2　并行传输与串行传输

**1. 并行传输**

并行传输是构成字符的多个数据位在并行信道上同时传输的方式。例如，8 位代码的字符要用 8 条信道并行同时传输，还可附加一位数据校验位（如图 3-5），一次即可传一个字符，收、发双方不存在字符同步问题。并行传输速度快，但信道多、投资大，主要用于近距离通信，不适于做较长距离的通信。最典型的例子是计算机和并行打印机之间的通信，网络传输中很少采用。

**2. 串行传输**

串行传输是构成字符的二进制代码在一条信道上逐位传输的方式。按位发送，逐位接收，需要进行串并转换（如图 3-6）；同时还要确认字符，所以要采取同步措施。串行传输速度虽慢，但只需一条传输信道，投资小，易于实现，对于覆盖面极其广阔的公用电话系统来说具有更大的现实意义。

串行传输是计算机网络通信采取的一种主要方式。

## 3.2.3　异步传输与同步传输

在串行传输中，通信双方收发数据序列必须在时间上取得一致，这样才能保证接收的数据与发送的数据一致（即同步），有两种不同的同步方法。

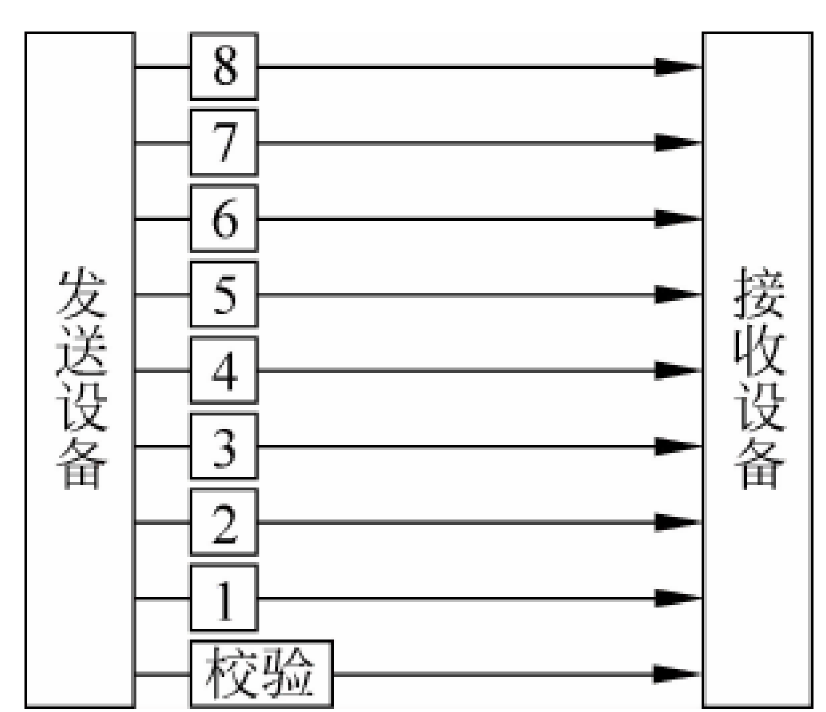



图 3-5 并行传输示意图

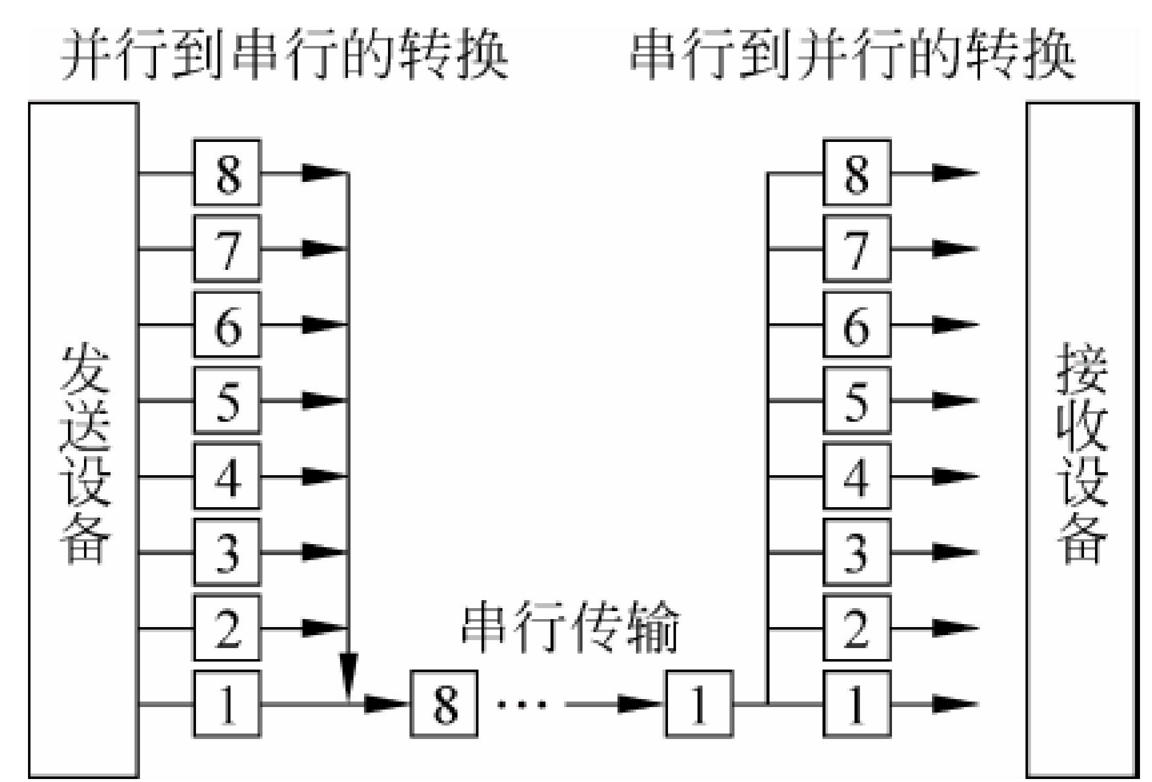



图 3-6 串行传输示意图

**1. 异步传输**

在异步传输中，被传输的任何两个字符之间间隔时间可以不同，但在一个字符时间之内，收发双方各数据位必须同步。发送方每传送一个字符都要在字符前加 1 个起始位，表示字符的开始，在字符代码和校验码后加 1 或 2 个停止位，表示字符的结束；接收方根据起始位或停止位判断一个字符开始或结束。这种传输方式又称为起-止式同步。

异步传输是面向字符的传输，传输的单位是字符；异步传输对时序的要求较低，每个字符之间的时间间隔是任意的；由于每个字符都需要多使用 2 或 3 个二进制位，增加了通信的开销，因而传输效率较低，适合于低速通信。

**2. 同步传输**

同步传输是面向比特的传输，传输的单位是带格式的数据块（帧）。在数据块之前先发送一个或多个同步字符 SYN，用于接收方进行同步检测，从而使通信双方进入同步状态；在同步字符之后，可以连续发送多个字符或数据块，发送完毕，再使用同步字符来标识整个发送过程结束。

同步传输通常要比异步传输快得多，因为接收方不必对每个字符进行开始和停止的操作。一旦检测到帧同步字符，它就在接下来的数据到达时接收它们。另外，同步传输的开销也比较少，适合于高速通信。

### 3.2.4 单工、半双工和全双工传输

在数据通信系统中，根据通信双方的分工和数据传输方向可将数据传输方式分为三种：单工、半双工和全双工，如图 3-7 所示。在计算机网络中主要采用双工方式。

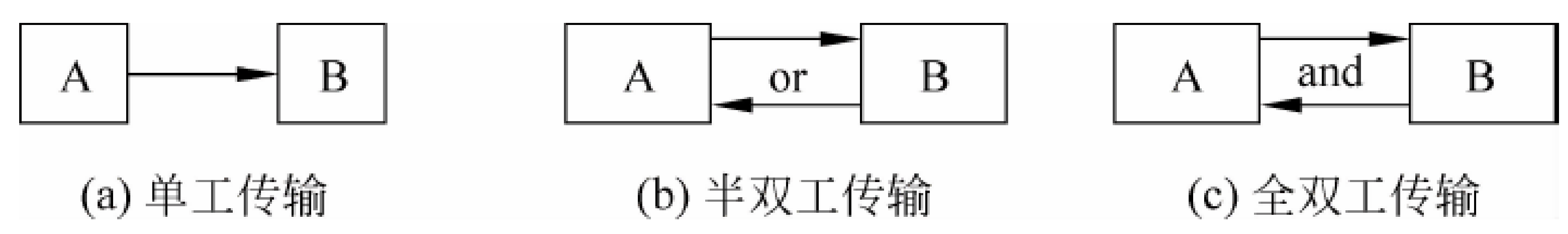



图 3-7 单工、半双工和全双工传输

**1. 单工传输**

单工传输只支持数据在一个方向上传输，任何时候都不能改变传输方向。例如，在家中收看电视节目。单工传输不适用于网络通信系统。

**2. 半双工传输**

半双工传输是指接收与发送共用一个载波信道，数据可以沿两个方向传送，但同一时刻只能发送或只能接收数据的传输方式。它实际上是一种切换方向的单工通信。

由于这种方式要频繁变换信道方向，故效率低，但可以节约传输线路。早期的对讲机以及早期集线器等设备都是基于半双工传输的产品。随着技术的不断进步，半双工传输会逐渐退出历史舞台。

**3. 全双工传输**

全双工传输是指在发送数据的同时也能够接收数据，两者同步进行，就像我们平时打电话一样，说话的同时也能够听到对方的声音。全双工数据传输是通过两个信道完成的，它相当于将两个方向相反的单工通信方式组合起来。

全双工传输效率高，控制简单，但造价高，适用于计算机之间的通信。目前的网卡、交换机一般都支持全双工传输。

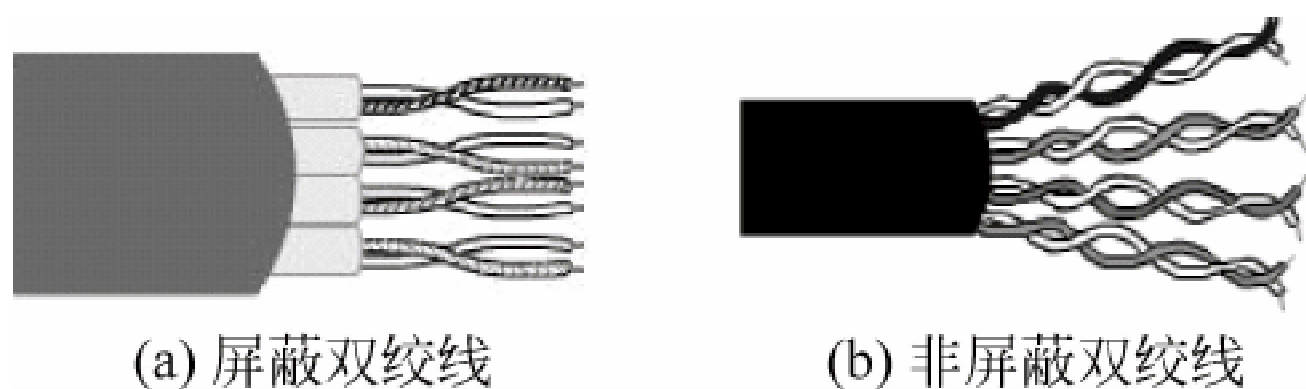
## 3.3　传输介质及其主要特性

传输介质分为有线和无线两大类。双绞线、同轴电缆和光纤是常用的三种有线传输介质；无线电、微波、红外以及激光则属于无线传输介质。传输介质的特性对网络数据通信质量有很大影响，应根据需要正确选择。

### 3.3.1　双绞线

双绞线是指两根螺旋状绞在一起的绝缘铜线，多个线对再按照一定的纽距绞在一起。多个双绞在一起的线对外面包裹着一层绝缘防护套，即构成双绞线电缆。计算机网络中双绞线一般用于数字信号传输。

双绞线电缆分为非屏蔽双绞线和屏蔽双绞线。屏蔽双绞线（Shielded Twisted Pair，STP）的每个线对带有屏蔽层（图 3-8（a）），所以抗干扰性好，性能高，用于远程中继线时，最大距离可以达到十几千米；但 STP 成本较高，所以一直没有广泛使用。屏蔽电缆在欧洲国家应用比较广泛。



(a) 屏蔽双绞线　　(b) 非屏蔽双绞线

图 3-8　双绞线

非屏蔽双绞线(Unshielded Twisted Pair,UTP)是指不带屏蔽层的电缆,表皮内包含的线对数量不定,但最常见的是 4 对,每一线对都由特定的颜色代码标识(图 3-8(b))。常见的 UTP 电缆包括 5 类、超 5 类以及 6 类线,传输距离一般不超过 100 米。由于 UTP 电缆成本低、带宽高,而且安装容易,目前在局域网中被广泛使用。如标准以太网 10BASE-T 和快速以太网 100BASE-T 就是使用 UTP 的,分别提供 10Mb/s 和 100Mb/s 的传输速率。

### 3.3.2 同轴电缆

同轴电缆由"同轴"的内外两个导体组成,最里层是内芯,向外依次为绝缘层、屏蔽层、塑料外套,内芯和屏蔽层构成一对导体。如图 3-9 所示。同轴电缆分为基带同轴电缆(阻抗 50Ω)和宽带同轴电缆(阻抗 75Ω)。

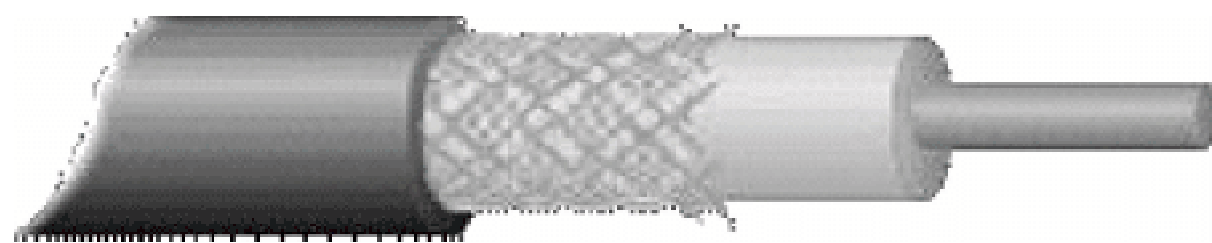


图 3-9 同轴电缆

基带同轴电缆又可分为粗缆和细缆两种,都用于直接传输数字信号,数据传输速率最高可达 10Mb/s。基带 50Ω 电缆每段可支持几百台设备,在大系统中还可以用转接器将各段连接起来,最大距离限制在几千米,在同样数据速率条件下,粗缆的传输距离较细缆的长。

宽带同轴电缆用于频分多路复用的模拟信号传输,也可用于不使用频分多路复用的高速数字信号和模拟信号传输。宽带 75Ω 电缆可以支持数千台设备,但在高数据传输率下(50Mb/s)使用宽带电缆时,设备数目限制在 20~30 台。宽带电缆的传输距离可达几十千米。闭路电视所使用的 CATV 电缆就是宽带同轴电缆。在同轴电缆上使用频分多路复用技术可以支持大量的视、音频通道。

与双绞线相比,同轴电缆的抗干扰能力强,数据传输能力大,但是由于同轴电缆安装和维护麻烦,而且成本更高,大多数局域网仍使用双绞线作为其首选的传输介质。

### 3.3.3 光导纤维

光导纤维简称光纤,由能传导光信号的石英玻璃纤维加保护层构成。光纤不受电磁干扰的影响,适于干扰很强的环境中;光纤支持很高的带宽,数据传输率可达 Gb/s 级;传输距离达数十千米,十分适合于高速数据主干线。每条光纤线路实际上都包含两根光缆。一根用于发送,另一根用于接收,如图 3-10 所示。

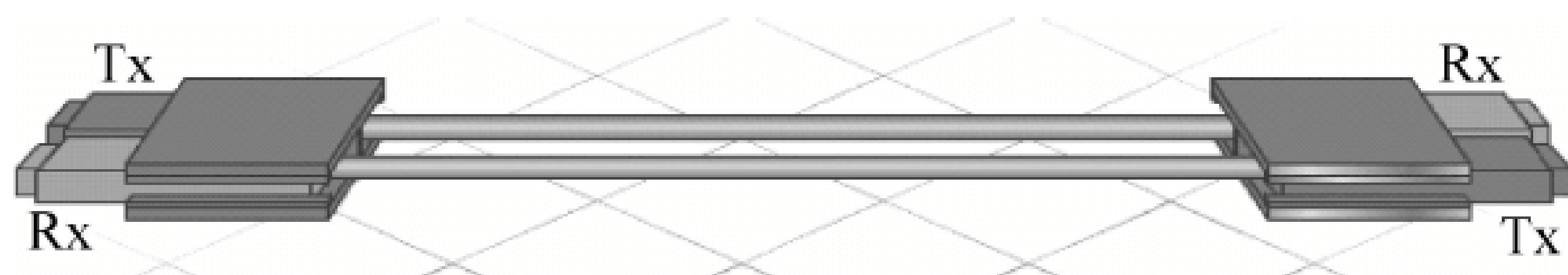



图 3-10 光纤线路示意图

光纤分为单膜光纤和多膜光纤两种，两种光纤工作在不同的波长区。光纤有三个工作波长区：0.85μm(微米)、1.3μm 和 1.55μm 波长区。其中 0.85μm 波长区为多模光纤通信方式，1.55μm 波长区为单模光纤通信方式，1.3μm 波长区有多模和单模两种方式。

单模光纤具备 10μm 的芯径，只能传一种光，且光束只能沿纤芯直线通行，如图 3-11(a)所示。单模光缆的光源通常为 LED 激光，另外，单模光纤怕弯曲，对熔接要求较高，很容易产生附加损耗。单模光纤成本高，数据传输快，传输距离长，约为 3000 米，通常用于主干、大容量、长距离的系统。

多模光纤的纤芯直径为 50μm 至 100μm，可传输多种光，光信号在纤芯内折线通行，如图 3-11(b)所示。多模光纤生成光脉冲的光源一般是 LED 可见光，其成本较低，性能比单模光纤差。但由于多模光纤易于安装和维护，成本低，广泛应用于小容量、短距离的系统中，一般适用于长度在 2000 米以内的链路。




图 3-11　光纤结构示意图

### 3.3.4　无线传输媒体

无线传输媒体不需要架设或铺埋线缆，比较适合于特殊场合下的数据传输。目前常用的无线媒体有无线电波、微波、红外线和激光。

微波是无线电波的一种，微波通信的载波频率为 2～40GHz 范围。由于工作频率很高，与通常的无线电波不一样，微波是沿直线传播的。直接传播的距离与天线的高度有关，天线越高传播距离越远，超过一定距离后就要用中继站来接力。由于地球表面是曲面，微波在地面的传播距离有限。

红外通信和激光通信也像微波通信一样，有很强的方向性，都是沿直线传播的。这三种技术都需要在发送方和接收方之间有一条视线通路，故它们统称为视线媒体。所不同的是，红外通信和激光通信把要传输的信号分别转换为红外光信号和激光信号直接在空间传播。

这三种视线媒体由于都不需要铺设电缆，对于连接不同建筑物内的局域网特别有用。这三种技术对环境气候较为敏感，例如雨、雾和雷电。相对来说，微波对一般雨和雾的敏感度较低。

### 3.3.5　传输媒体的选择

传输媒体的选择取决于以下诸因素：网络拓扑的结构、实际需要的通信容量、可靠性要求、能承受的价格范围。

双绞线的显著特点是价格便宜,但与同轴电缆相比,其带宽受到限制。对于单个建筑物内的低通信容量局域网来说,双绞线的性能价格比可能是最好的。

同轴电缆的价格要比双绞线贵一些,对于大多数的局域网来说,需要连接较多设备而且通信容量相当大时可以选择同轴电缆。

光纤作为传输媒体,与同轴电缆和双绞线相比具有一系列优点:频带宽、速率高、体积小、重量轻、衰减小、能电磁隔离、误码率低等。因此,在国际和国内长话传输中的地位日益提高,并已广泛用于高速数据通信网。随着光纤通信技术的发展和成本的降低,光纤作为局域网的传输媒体也得到了普遍采用,光纤分布数据接口 FDDI 就是一例。

## 3.4 数据交换技术

数据通信网络中的两个端系统之间不是直通专线连接的时候,通常需要通信子网中多个网络节点的转接,这种实现端系统之间接通数据通路的转接技术就是数据交换技术。通常,网络系统所采用的数据传输技术有以下三种:电路交换、报文交换和分组交换。

### 3.4.1 电路交换

电路交换是指在通信之前双方建立一条被独占的物理通路,该通路由通信双方之间的交换设备和链路逐段连接而成,通信结束后该通路被拆除,即电路交换包括电路建立、数据传输、电路拆除三个阶段。电路交换的运作方式类似于通过电话网络拨打电话。

电路交换的优点是:链路专用、数据直达,传输数据时延小;链路建立后,双方可以随时通信,实时性强;按发送顺序传送数据,不存在失序问题,适用于交互式会话通信。

电路交换的缺点是:需要额外的电路建立时间;连接建立后,物理通路被通信双方独占,即使通信线路空闲,也不能供其他用户使用,因而信道利用率较低;而且,电路交换时数据直达,不同类型、不同规格、不同速率的终端很难相互进行通信,也难以在通信过程中进行差错控制。

电路交换适于数据传输要求质量高,批量大的情况。典型的是电话通信网络,ISDN 或拨号连接便属于电路交换。

### 3.4.2 报文交换

报文交换不需要先建立专用通路,发送方在发送一个报文时把目的地址附加在报文上,途经的节点根据报文上的地址信息,将报文转发到下一个节点,接力式的完成整个传送过程。数据传送过程采用存储-转发的方式,每个节点在收到报文后,会将其暂存并检查有无错误,然后通过路由信息找出适当路线的下一个节点的地址,再把报文传送给下一个节点。

这个过程中,报文的传输只是占用两个节点之间的一段线路,而其他路段可传输其他用

户的报文。于是，报文交换不会像电路交换占用终端间的全部信道，提高了信道利用率。但是，报文在经过节点时会产生延迟。这段延迟包括接收报文所有位(b)所需的时间、等待时间和发送到下一个节点所需的排队延迟。

相对于电路交换，报文交换的优点有：信道利用率高；节点可暂存报文并对报文进行差错控制和码制转换；电路交换网络中，通信量很大时将不能接收某些信息，但在报文交换网络中却仍然可以，只是延迟会大些；可以方便地把报文发送到多个目的节点；建立报文优先权，让优先级高的报文优先传送。

报文交换也存在缺点：由于采用了完整报文的存储/转发，使得在交换节点的存储/转发时延较长，从而增加了网络传输的延迟，不利于实现交互性通信。

### 3.4.3　分组交换

分组交换仍采用存储-转发的传输方式，但将一个长报文先分割为若干个较短的分组，然后把这些分组(携带源、目的地址和编号信息)逐个地发送出去，传输过程和报文交换类似，只是由于限制了每个分组的长度，减轻了节点负担，改善了网络传输性能。

分组交换是计算机网络中使用最广泛的一种交换技术，分为数据报分组交换和虚电路分组交换两种。帧中继便是一种典型的虚电路分组交换网络。

**1. 数据报分组交换**

数据报分组交换是指同一报文的不同分组在传输过程中都带有源节点和目的节点地址，由不同的传输路径通过通信子网。分组到达目的节点时可能出现乱序、重复或丢失的现象，因此，在到达接收站之后还需对数据报分组进行排序重组。使用数据报方式时，数据报文传输延迟较大，适用于突发性通信，不适用于长报文和会话式通信。

**2. 虚电路分组交换**

虚电路分组交换是两个用户的终端设备在开始互相发送数据之前，需要通过通信网建立虚电路，发送数据时，所有的分组都沿着这条虚电路按顺序传送，用户不需要在发送和接收数据时清除连接。

虚电路分组交换方式也包括虚电路建立、数据传输、虚电路拆除三个阶段，传输时，报文分组不必带目的地址、源地址等辅助信息，只需要携带虚电路标识号。报文分组通过每个虚电路上的节点时，节点只需要做差错控制，而不需要做路径选择。通信子网中的每个节点都可以和任何节点建立多条虚电路连接。

虚电路分组交换方式具有分组交换与电路交换两种方式的优点。它加速了数据在网络中的传输，简化了存储管理，减少了出错概率和重发数据量；由于分组短小，更适用于采用优先级策略，便于及时传送一些紧急数据，因此对于计算机之间的突发式的数据通信，分组交换显然更为合适些。

## 思考与练习

### 一、填空题

1. 数据通信系统由________、________和________组成。

2. 数据通信系统中，信息、数据和信号含义不同而又相互关联。________是指数据的内容和解释，________是数据的电子或电磁编码。

3. ________是指单位时间内信道上所能传输的数据量，可用________和________来表示。

4. 多路复用技术包括________、________、________和码分多路复用 CDM。

5. 按被传输的数据信号的特点，数据传输可分为________、________和宽带传输；按数据传输的顺序可分为________和________；按数据传输的流向和时间可分为________、________和________传输；按数据传输的同步方式可分为________和________。

6. 传输介质分为有线和无线两大类：________、________和________是常用的三种有线传输介质；无线电、微波、红外以及激光则属于无线传输介质。

7. 具有分组交换与电路交换两种方式优点的数据交换技术是________。

### 二、选择题

1. 以下不属于网络 DTE 设备是(　　)。

A. 计算机　　B. 路由器　　C. 交换机　　D. 网络打印机

2. 信源发出的没有经过调制的原始电信号所固有的频带称为(　　)。

A. 频带　　B. 基带　　C. 宽带　　D. 带宽

3. 以下不属于多路复用技术的是(　　)。

A. FDM　　B. SDM　　C. TDM　　D. CDM

4. 以下属于串行传输特点的是(　　)。

A. 每次传输一个字节　　B. 每次传输一个比特

C. 速度快　　D. 不需要进行串并转换

5. 以下属于全双工通信的是(　　)。

A. 看电视　　B. 无线对讲机　　C. 听广播　　D. 网络聊天

6. 以下不属于非屏蔽双绞线 UTP 特性的是(　　)。

A. 抗干扰能力强　　B. 价格便宜

C. 在局域网中广泛使用　　D. 最大传输距离是 100 米

7. 以下不属于光纤工作波长区的是(　　)。

A. 0.85$\mu$m　　B. 1.3$\mu$m　　C. 50$\mu$m　　D. 1.55$\mu$m

8. 以下不属于无线传输介质的是(　　)。

A. 光纤　　B. 微波　　C. 红外线　　D. 卫星

9. 数据传输期间，物理通路被独占的数据交换技术是(　　)。
   A. 电路交换　　B. 报文交换
   C. 数据报分组交换　　D. 虚电路分组交换

10. 需要经历虚电路建立、数据传输、虚电路拆除三个阶段的数据交换技术是(　　)。
   A. 电路交换　　B. 报文交换
   C. 数据报分组交换　　D. 虚电路分组交换

**三、思考题**

1. 什么是多路复用，有哪些常见的多路复用技术？
2. 基带传输与宽带传输的差别是什么？
3. 同步传输与异步传输有什么不同？
4. 比较三种有线传输媒体，如何选择传输媒体？
5. 比较电路交换、报文交换和分组交换的不同。

第 4 章

# 局　域　网

个人计算机的发展和普及促进了局域网的形成。局域网可以实现文件管理、应用软件共享、打印机共享、扫描仪共享、工作组内的日程安排、电子邮件和传真通信服务等功能。局域网是封闭型的,可以由办公室内的两台计算机组成,也可以由一个公司内的上千台计算机组成。在当今的计算机网络技术中,局域网技术已经占据十分重要的地位。

## 4.1　局域网概述

局域网(LAN)是在一个有限的地理范围内(如一个学校、工厂和机关内),将各种计算机、外部设备和数据库等互相连接起来组成的计算机通信网。它可以通过数据通信网或专用数据电路,与远方的局域网、数据库或处理中心相连接,构成一个大范围的信息处理系统,简称 LAN。

局域网是连接范围最小的网络,也是目前应用最为广泛及技术发展最快的数据通信系统。从定义上讲,局域网是一种通信网络,如使用电话交换机的小型电话交换网也属于局域网。而本章所介绍的局域网则侧重于计算机局域网,即主要指在一个有限范围内将多个独立的计算机系统连接起来,并在相关软件的支持下,实现系统资源共享的计算机网络系统,即计算机局域网。

### 4.1.1　局域网的特点及分类

**1. 局域网的主要特点**

局域网的特点除了具备结构简单、数据传输率高,可行性高,实际投资少且技术更新发展迅速等基本特征外,还具有以下特点:

(1) 具有较高的数据传输速率(通常为 10～100Mb/s),目前速率高达上千 Mb/s 的局域网也已经广泛使用,可交换各类数字和非数字(如语音、图像、视频等)信息。

(2) 具有优良的传输质量,误码率低。局域网通常采用短距离基带传输,可以使用高质量的传输介质,从而提高数据传输质量。误码率一般为 $10^{-11}$～$10^{-8}$。

(3) 具有对不同速率的适应能力,低速或高速设备均能接入。

(4) 具有良好的兼容性和互操作性,不同厂商生产的不同型号的设备均能接入。

(5) 支持多种同轴电缆、双绞线、光纤和无线等多种传输介质。

(6) 网络覆盖范围有限，一般为 0.1～10km。一般为一个单位或部门所独有，协议简单、结构灵活、便于管理和扩充。

**2. 局域网的分类**

按照不同的划分标准，可以对局域网进行多种分类，常见的有如下几种：

(1) 按照网络的拓扑结构分，可以分为星型局域网、总线型局域网、环形局域网。

(2) 按照网络的传输介质分，可以分为双绞线局域网、同轴电缆局域网、光纤局域网、无线局域网。

(3) 按照网络的介质访问控制方式分，可以分为以太网、令牌环网、令牌总线网。

(4) 按照传输的信号来分，可分为基带局域网和宽带局域网。

(5) 按照服务的对象来分，可以将局域网分为企业网、校园网等类型。

### 4.1.2　局域网体系结构与 IEEE 802 标准

OSI 参考模型是具有一般性的网络模型结构，它作为一种标准框架为构建网络提供了一个参照系。但局域网作为一种特殊的网络，有它自身的技术特点。而且由于局域网实现方法的多样性，所以它并不完全套用 OSI 体系结构。

国际上通用的局域网标准由 IEEE 802 委员会制定。IEEE 802 委员会根据局域网适用的传输介质、网络拓扑结构、性能及实现难易等因素，为局域网制定了一系列标准，称为 IEEE 802 标准，目前，许多 IEEE 802 标准已被 ISO 采纳为国际标准。局域网的相关标准和规范由 OSI 的最低两层(物理层和数据链路层)来定义。局域网的数据链路层又划分为介质访问控制(Medium Access Control，MAC)子层和逻辑链路控制(Logical Link Control，LLC)两个子层。网络的服务访问点 SAP 在 LLC 子层与高层的交界面上，而与各种接入传输介质有关的问题都放在 MAC 子层。MAC 子层还负责在物理层的基础上进行无差错的通信。

**1. MAC 子层的主要功能**

(1) 上层交下来的数据封装成帧进行发送(接收时进行相反的过程，将帧拆卸)。

(2) 实现和维护 MAC 协议。

(3) 比特差错检测。

(4) 寻址。

数据链路层中与介质接入无关的部分都集中在逻辑链路控制 LLC 子层。

**2. LLC 子层的主要功能**

(1) 建立和释放数据链路层的逻辑连接。

(2) 提供与高层的接口。

(3) 差错控制。

(4) 给帧加上序号。

局域网对 LLC 子层是透明的。

**3. IEEE 802 系列标准**

IEEE 802 委员会为局域网制定了一系列标准，它们统称为 IEEE 802 标准。IEEE 802 标准包括以下内容。

（1）IEEE 802.1 标准：定义了局域网体系结构、网络互联以及网络管理和性能测试。

（2）IEEE 802.2 标准：定义了逻辑链路控制（LLC）子层的功能与服务。

（3）IEEE 802.3 标准：定义了 CSMA/CD 总线介质访问控制子层与物理层规范。

（4）IEEE 802.4 标准：定义了令牌总线（Token Bus）介质访问控制子层与物理层规范。

（5）IEEE 802.5 标准：定义了令牌环（Token Ring）介质访问控制子层与物理层规范。

（6）IEEE 802.6 标准：定义了城域网介质访问控制子层与物理层规范。

（7）IEEE 802.7 标准：定义了宽带网络技术。

（8）IEEE 802.8 标准：定义了光纤传输技术。

（9）IEEE 802.9 标准：定义了综合语音与数据局域网（Integrated Voice Data LAN，IVD LAN）技术。

（10）IEEE 802.10 标准：定义了可互操作的局域网安全性规范（Standardfor Interoperable LAN Security，SILS）。

（11）IEEE 802.11 标准：定义了无线局域网介质访问控制方法和物理层规范。

（12）IEEE 802.12 标准：定义了 100VG-Any LAN 访问控制方法和物理层技术规范。

（13）IEEE 802.13 标准：未使用。

（14）IEEE 802.14 标准：定义了交互式电视网（Cable Modem）技术。

（15）IEEE 802.15 标准：定义了无线个人局域网（Wireless Personal Area Network Communi Cation，WPAN）的 MAC 子层和物理层规范。

（16）IEEE 802.16 标准：定义了宽带无线城域网标准（Broadband Wireless MAN Standard）。

（17）IEEE 802.17 标准，正在制定的弹性分组环（Resilient Packet Ring，RPR）标准。

（18）IEEE 802.18 标准，正在制定的宽带无线局域网标准规范。

### 4.1.3 局域网的关键技术

局域网的特性主要涉及三项技术问题，分别是连接各种设备的拓扑结构、传输介质和介质访问控制方式。其中最重要的是介质访问控制。这三种技术在很大程度上决定了传输数据的类型、网络的响应时间、吞吐量、负载特性等各种网络特征。

**1. 局域网的拓扑结构**

计算机网络拓扑结构是指网络中各个站点间相互连接的形式。在局域网中就是文件服务器、工作站、网络设备和电缆等的连接形式。通俗地讲，就是这些网络设备是如何连接在一起的。目前，局域网常见的网络拓扑结构主要有以下 4 大类。

1）星型结构

星型网由通过点到点链路接到中央节点的各站点组成的，通过中心设备实现许多点到点连接。在数据网络中，这种设备是主机或集线器。在星型网中，可以在不影响系统其他设备工作的情况下，非常容易地增加和减少设备。

星型拓扑的优点是：利用中央节点可方便地提供服务和重新配置网络；单个连接点的故障只影响一个设备，不会影响全网，容易检测和隔离故障，便于维护；任何一个连接只涉及中央节点和一个站点，因此控制介质访问的方法很简单，从而访问协议也十分简单。

星型拓扑的缺点是：每个站点直接与中央节点相连，需要大量电缆，因此费用较高；如果中央节点产生故障，则全网不能工作，所以对中央节点的可靠性和冗余度要求很高。

星型结构是目前在局域网中应用得最为普遍的一种，在企业网络中几乎都是采用这一方式。星型网络几乎是 Ethernet（以太网）网络专用，它是因网络中的各节点设备通过一个网络集中设备（如集线器或者交换机）连接在一起，各节点呈星状分布而得名。这类网络目前用得最多的传输介质是双绞线，如常见的 5 类和超 5 类双绞线等。

2）环形结构

由连接成封闭回路的网络节点组成，每一节点与它左右相邻的节点连接。环形网络的一个典型代表是令牌环局域网，它的传输速率为 4Mb/s 或 16Mb/s，这种网络结构最早由 IBM 推出，但现在被其他厂家采用。在令牌环网络中，拥有“令牌”的设备允许在网络中传输数据。这样可以保证在某一时间内网络中只有一台设备可以传送信息。在环形网络中信息流只能是单方向的，每个收到信息包的站点都向它的下游站点转发该信息包。信息包在环网中“旅行”一圈，最后由发送站进行回收。

环形结构的网络形式主要应用于令牌网中，在这种网络结构中各设备是直接通过电缆来串接的，最后形成一个闭环，整个网络发送的信息就是在这个环中传递，通常把这类网络称之为“令牌环网”。实际上大多数情况下这种拓扑结构的网络不会是所有计算机真的要连接成物理上的环形，一般情况下，环的两端是通过一个阻抗匹配器来实现环网的封闭的，因为在实际组网过程中因地理位置的限制而不方便真正做到环的两端物理连接。

3）总线型结构

总线型网络采用单根传输线作为传输介质，所有的站点都通过相应的硬件接口直接连接到传输介质（或称总线）上。使用一定长度的电缆将设备连接在一起。设备可以在不影响系统中其他设备工作的情况下从总线中取下。任何一个站点发送的信号都可以沿着介质传播，而且能被其他所有站点接收。

总线拓扑的优点是：电缆长度短，易于布线和维护；结构简单，传输介质又是无源元件，从硬件的角度看，十分可靠。

总线拓扑的缺点是：因为总线拓扑的网不是集中控制的，所以故障检测需要在网上的各个站点上进行；在扩展总线的干线长度时，需重新配置中继器、剪裁电缆、调整终端器等；总线上的站点需要介质访问控制功能，这就增加了站点的硬件和软件费用。

总线型网络拓扑结构中所有设备都直接与总线相连，它所采用的介质一般也是同轴电缆（包括粗缆和细缆），不过现在也有采用光缆作为总线型传输介质的，如 ATM 网、Cable Modem 所采用的网络等都属于总线型网络结构。

4）树型结构

树型结构是总线型结构的扩展，它是在总线网上加上分支形成的，形状像一棵倒置的树，节点按层次连接，信息交换主要在上下节点之间进行，相邻节点或同层节点之间一般不进行数据交换。其传输介质可有多条分支，但不形成闭合回路。树型网是一种层次结构，其结构可以对称，联系固定，具有一定的容错能力，一般一个分支和节点的故障不影响另一分支节点的工作，任何一个节点送出的信息都可以传遍整个传输介质，也是广播式网络。一般树型网上的链路相对具有一定的专用性，无须对原网做任何改动就可以扩充工作站。

**2. 局域网的传输介质**

连接网络首先要用的东西就是传输线，它是组建网络的最低要求。常见的传输线有 4 种基本类型：同轴电缆、双绞线、光纤和无线电波。每种类型都满足了一定的网络需要，都解决了一定的网络问题。

同轴电缆的中央是铜芯，铜芯外包着一层绝缘层，绝缘层外是一层屏蔽层，屏蔽层将电线很好地包起来，再往外就是外包皮了。由于同轴电缆的这种结构，它对外界具有很强的抗干扰能力。同轴电缆是局域网最普遍使用的传输媒体。

在局域网中，双绞线用得非常广泛，这主要是因为其低成本、高速度和高可靠性。双绞线有两种基本类型：屏蔽双绞线（STP）和非屏蔽双绞线（UTP），它们都是由两根绞在一起的导线而形成传输电路。两根导线绞在一起主要是为了防止干扰（线对上的差分信号具有共模抑制干扰的作用）。

有些网络应用要求很高，需可靠、高速地长距离传送数据，在这种情况下，光纤就是一个理想的选择。光纤具有圆柱形的形状，由 3 部分组成：纤芯、包层和护套。纤芯位于最内层，它由一根或多根非常细的由玻璃或塑料制成的绞合线或纤维组成。每一根纤维都由各自的包层包着。包层是玻璃或塑料涂层，它具有与纤芯不同的光学特性。最外层是护套，它包着一根或一束已加包层的纤维。护套是由塑料或其他材料制成的，用于防止潮气、擦伤、压伤或其他外界带来的危害。

传输线系统除同轴电缆、双绞线和光纤外，还有一种手段是根本不使用导线，这就是无线电通信。无线电通信利用电磁波或光波来传输信息，使用它不用铺设缆线就可以把网络连接起来。无线电通信包括两个独特的网络：无线 LAN 网络和移动网络。利用无线 LAN 网，机器可以通过发射机和接收机连接起来；利用移动网络，机器可以通过蜂窝式通信系统连接起来，该通信系统由无线电通信部门提供。

**3. 局域网的介质访问控制方式**

介质访问控制方法是局域网最重要的一项基本技术，对局域网体系结构、工作过程和网络性能产生决定性影响。将传输介质的频带有效地分配给网上各节点的方法称为介质访问

控制方法。它主要解决介质使用权的算法或机构问题，如何使众多用户能够合理而方便地共享通信介质资源，从而实现对网络传输信道的合理分配。

介质访问控制方法的主要内容有两个方面：一是要确定网络上每一个节点能够将信息发送到介质上去的特定时刻；二是要解决如何对共享介质访问和利用加以控制。局域网常用的介质访问控制方法有三种：总线结构的具有冲突检测的载波侦听多路访问 CSMA/CD 方法、环形结构的令牌环访问控制方法和令牌总线访问控制方法。

1）具有冲突检测的载波侦听多路访问（CSMA/CD）控制方法

CSMA/CD(Carrier Sense Multiple Access/Collision Detection)是采用争用技术的一种介质访问控制方法。CSMA/CD 通常用于总线型拓扑结构和星型拓扑结构的局域网中。IEEE 802.3(以太网)是一种总线型局域网，使用的介质访问控制方法就是 CSMA/CD。

CSMA/CD 的每个节点都能独立决定发送帧，若两个或多个节点同时发送，即产生冲突。把在一个以太网中所有相互之间可能发生冲突的节点的集合称为一个冲突域。当一个冲突域中的节点数目过多时，冲突就会很频繁。因此，在以太网中节点数目过多将会严重影响网络性能。为了避免数据传输的冲突，以太网采用 CSMA/CD 机制规范节点对共享信道的使用。每个节点都能判断是否有冲突发生，如冲突发生，则等待随机时间间隔后重发，以避免再次发生冲突。CSMA/CD 的工作原理可概括为四句话：先听后发，边发边听，冲突停止，随机延时后重发。具体过程如下。

（1）当一个节点想要发送数据的时候，它首先检测网络是否有其他节点正在传输数据，即侦听信道是否空闲。

（2）如果信道忙，则等待，直到信道空闲。

（3）如果信道闲，节点就传输数据。

（4）在发送数据的同时，节点继续侦听网络确信没有其他节点在同时传输数据。因为有可能两个或多个节点都同时检测到网络空闲然后几乎在同一时刻开始传输数据。如果两个或多个节点同时发送数据，就会产生冲突。

（5）当一个传输节点识别出一个冲突，它就发送一个拥塞信号，这个信号使得冲突的时间足够长，让其他的节点都能发现。

（6）其他节点收到拥塞信号后，都停止传输，等待一个随机产生的时间间隙（回退时间 Back off Time）后重发。

总之，CSMA/CD 采用的是一种“有空就发”的竞争型访问策略，因而不可避免会出现信道空闲时多个节点同时争发的现象，无法完全消除冲突，只能是采取一些措施减少冲突，并对产生的冲突进行处理。因此采用这种协议的局域网环境不适合于对实时性要求较强的网络应用。

2）令牌环访问控制方法

Token Ring 是令牌传送环（Token Passing Ring）的简写。令牌环网最早起源于 IBM 于 1985 年推出的环形基带网络。IEEE 802.5 标准定义了令牌环网的国际规范。令牌环介

质访问控制方法是通过在环形网上传输一种称之为“令牌(Token)”的短帧的方式来实现对介质的访问控制。只有拥有令牌的节点才有权发送信息。

令牌平时不停地在环路上流动,当一个节点有数据要发送时,必须等到令牌出现在本节点时截获它,即将令牌的独特标志转变为信息帧的标志(或称把闲令牌置为忙令牌),然后将所要发送的信息附在该令牌之后发送出去。在环上传输的信息逐个节点不断向前传输,一直到达目的节点。目的节点一方面复制这个帧(即收下这个帧),另一方面还要将此信息帧转发给下一个节点(并在其后附上已接收标志)。信息在环路上转了一圈后回到源节点,源节点对返回的数据进行检查,查看本次发送是否成功。同时,源节点必须生成一个新的令牌,将令牌发送给下一个节点,环路上又有令牌在流动,等待着某个节点去截获它。总之,截获令牌的节点要负责在发送完信息后再将令牌恢复出来,发送信息的节点要负责从环路上收回它所发出的信息。归纳起来,令牌环网主要有下面三种操作:

(1) 截获令牌并且发送数据帧。如果没有节点需要发送数据,令牌就由各个节点沿固定的顺序逐个传递;如果某个节点需要发送数据,它要等待令牌的到来,当空闲令牌传到这个节点时,该节点修改令牌帧中的标志,使其变为“忙”的状态,然后去掉令牌的尾部,加上数据,成为数据帧,发送到下一个节点。

(2) 接收与转发数据。数据帧每经过一个节点,该节点就比较数据帧中的目的地址,如果不属于本节点,则转发出去;如果属于本节点,则复制到本节点的计算机中,同时在帧中设置已经复制的标志,然后向下一节点转发。

(3) 取消数据帧并且重发令牌。当数据帧通过闭环重新传到发送节点时,发送节点不再转发,而是检查发送是否成功。如果发现数据帧没有被复制(传输失败),则重发该数据帧;如果发现传输成功,则清除该数据帧,并且产生一个新的空闲令牌发送到环上。

令牌环网采用的是单令牌策略,即环路上只能有一个令牌存在,只要有一个节点发送信息,环路上就不会再有空闲的令牌流动。这种策略可以保证任一时刻环路上只能有一个发送节点,不会出现像以太网那样的竞争局面,环网不会因发生冲突而降低效率。

与 CSMA/CD 不同,令牌传递网是延迟确定型网络。也就是说,在任何节点发送信息之前,可以计算出信息从源节点到目的节点的最长时间延迟。采用确定型介质访问控制方法的令牌环网最大的优点是适合于传输距离远、负载重和实时性要求严格的应用环境。其缺点是令牌传送方法实现较复杂,而且所需硬件设备也较为昂贵,网络维护与管理也较复杂。

3) 令牌总线访问控制方法

令牌总线访问控制方法是在物理总线上建立一个逻辑环,令牌在逻辑环路中依次传递,其操作原理与令牌环相同。该种方法是在综合了 CSMA/CD 和 Token Ring 两种介质访问方法优点的基础上,形成的一种简单、公平、性能良好的介质访问控制方法。

令牌总线网络中各节点共享的传输介质是总线型的,每一节点都有一个本节点地址,并知道上一个节点地址和下一个节点地址,令牌传递规定由高地址向低地址,最后由最低地址

向最高地址依次循环传递，从而在一个物理总线上形成一个逻辑环。与令牌环一致，只有获得令牌的节点才能发送数据。在正常工作时，当节点完成数据帧的发送后，将令牌传送给下一个节点。从逻辑上看，令牌是按地址的递减顺序传给下一个节点的。而从物理上看，带有地址字段的令牌帧广播到总线上的所有节点，只有节点地址和令牌帧的目的地址相符的节点才有权获得令牌。

由于总线上每一节点接收令牌的过程是按顺序依次进行的，因此所有节点都有访问权。为了使节点等待令牌的时间是确定的，需要限制每一节点发送数据帧的最大长度。如果所有节点都有数据要发送，则在最坏的情况下，等待获得令牌的时间和发送数据的时间应该等于全部令牌传送时间和数据发送时间的总和。另一方面，如果只有一个节点有数据要发送，则在最坏的情况下，等待时间只是令牌传送时间的总和，实际等待时间在这一区间范围内。

令牌总线还提供了不同的优先级机制。优先级机制的功能是将待发送的帧分成不同的访问类别，赋予不同的优先级，并把网络带宽分配给优先级较高的帧，而当有足够的带宽时，才发送优先级较低的帧。

令牌总线的特点在于它的确定性、可调整性及较好的吞吐能力，适用于对数据传输实时性要求较高或通信负荷较重的应用环境中，如生产过程控制领域。它的缺点在于它的复杂性和时间开销较大，节点可能要等待多次无效的令牌传送后才能获得令牌。

### 4.1.4　以太网的工作机制

20 世纪 70 年代和 80 年代出现了各种实验性的和商业化的局域网，如美国加州大学的 Newhall 环网、英国剑桥大学的剑桥环、3COM 的以太网、IBM 的令牌环以及 ArcNet 等。经过多年的市场考验，以太网终于以其技术成熟、连网方便、价格低廉等优点脱颖而出。以太网是当前占主导地位的分组交换局域网技术，是由 Xerox（施乐）公司的 PARC（Palo Alto Research Center）在 20 世纪 70 年代早期发明的。Xerox 公司、Intel 公司和 DEC 公司于 1978 年将以太网进行了标准化。后来 IEEE 参考该标准制订了 IEEE 802.3 标准。目前以太网已经成为了一种最流行的局域网技术。

最初的以太网设计采用总线结构，用同轴电缆作为传输介质，采用 CSMA/CD 的介质访问控制方式。以太网的传输介质经历了由粗同轴电缆到细同轴电缆，再到双绞线的发展过程，与之对应的网络拓扑结构也经历了由总线型到星型的发展过程。20 世纪 70 年代末以太网得到了标准化，对当时的计算机而言，10Mb/s 的工作速率可以完全满足需求。但到了 20 世纪 90 年代中期，计算机的能力迅速增强，为了克服以太网吞吐率的限制，人们设计了 100Mb/s 的新以太网版本（100Base-T），即快速以太网（Fast Ethernet）。20 世纪 90 年代末期，随着 100Base-T 以太网的普及，对以太网的吞吐能力的要求也不断提高。为了满足这一更大整体吞吐量的要求，人们又设计研究出了千兆位以太网。如今，传输速率达 10Gb/s 的万兆位以太网也已实现，是当前最先进的以太网技术。

**1. IEEE 802.3 标准系列和以太网**

1）IEEE 802.3 帧格式

无论是以太网，快速以太网，还是千兆以太网，其数据帧的格式都是一样的，因此，这三种网络可以方便地交换数据包。IEEE 802.3 以太网帧的格式如图 4-1 所示。

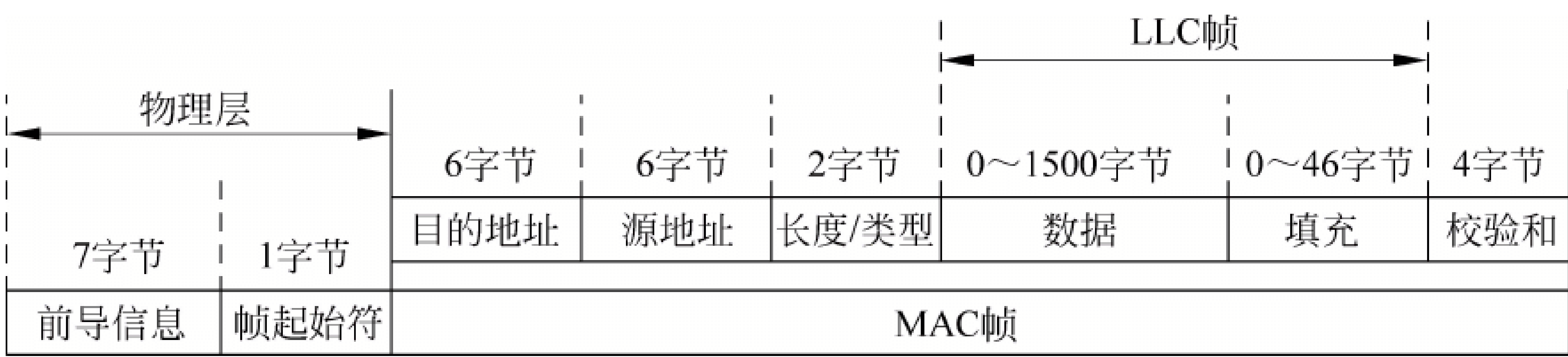



图 4-1　IEEE 802.3 帧格式

（1）前导信息和帧起始符：当 MAC 帧传送到物理层时要加上这两个字段，其中 7 字节的前导信息的每一个字节都由 10101010 组成，而 1 字节的帧起始符由 10101011 组成。其中，前导信息的作用是在接收端接收到 MAC 帧时能够迅速实现比特传输的同步，它通过曼彻斯特编码产生 10MHz、持续 5.6μs 的矩形波，作为接收端的同步信息。帧起始符表示前导信息结束，一个 MAC 帧开始。

（2）目的地址和源地址：IEEE 规定对 10Mb/s 基带以太网，此两个字段使用 6 字节的地址长度。目前地址最高位为 0 时表示单个地址，为 1 时表示组地址。全 1 的目的地址为广播地址，这时所有站点都会接收到该帧。

（3）长度/类型：数据长度（PDU 长度）字段说明后面数据字段的长度；帧类型字段决定将帧交给哪个协议软件模块进行处理（如果帧类型为 0x0800，则将数据交给上层的 IP 协议处理，如果帧类型为 0x0806，则将数据交给上层的 ARP 协议处理）。

（4）数据：IEEE 802.3 的字段长度在 0～1500 字节之间，它表示 LLC 子层传送下来的数据大小，即 LLC PDU 的大小。

（5）填充：由于数据字段可以为 0，这时帧中不包含任何 LLC 子层传来的数据。为了保证帧发送期间能够检测到可能发生的冲突，IEEE 802.3 标准规定最小帧长度为 64 字节。这里的最小帧长度是指上图中的目的地址、源地址、数据长度、数据、填充、校验和 6 个字段组成的总长度。由于前导信息和帧起始符是由物理层加上的，所以不包含在最小帧长度中，也不参与帧检验。如果最小帧长度不足 64 字节时，由填充位负责填充（内容不限）。

（6）校验和：负责对 MAC 帧进行差错校验，保证局域网中数据传输的误码率控制在 $10^{-11}$～$10^{-8}$之间。

IEEE 802.3 以太网帧是变长的，有效的 MAC 帧的大小在 64～1518 字节之间。当帧的大小不在此范围内，或帧的大小不是整数个字节时，接收端便认为该帧是错误帧或无效帧。MAC 子层不会将错误帧或无效帧上交给 LLC 子层进行处理，但会通知上层的网络管

理软件。当帧到达目的主机后，数据链路层协议对数据帧进行校验，解封装，并根据帧类型决定将帧交给哪个协议软件模块进行处理。如果帧类型为 0x0800，则将数据交给上层的 IP 协议处理；如果帧类型为 0x0806，则将数据交给上层的 ARP 协议处理。

2）以太网的地址

区别以太网设备的标识为 MAC 地址，它是每一个以太网设备的唯一标识，生产网络设备（如以太网网络接口卡、无线设备、路由器和交换机）的供应商预先把这些地址烧录到他们的设备中，以太网内的寻址就是 MAC 地址的寻址。MAC 地址还有一些其他的叫法，如物理地址、以太网地址和硬件地址。MAC 地址是一个由 12 个字符组成的十六进制字符串，总长度为 48b。其中 0～23 位是由厂家自己分配，24～47 位叫做组织唯一标志符（Organizationally Unique），是识别局域网节点的标识，其中第 40 位是组播地址标志位，当该位为 0 时表示单个地址，当该位为 1 时表示组地址，如 00-18-F3-C1-37-3E。

在 Windows 中，可以使用 ipconfig /all 命令查看 MAC 地址，如图 4-2 所示。

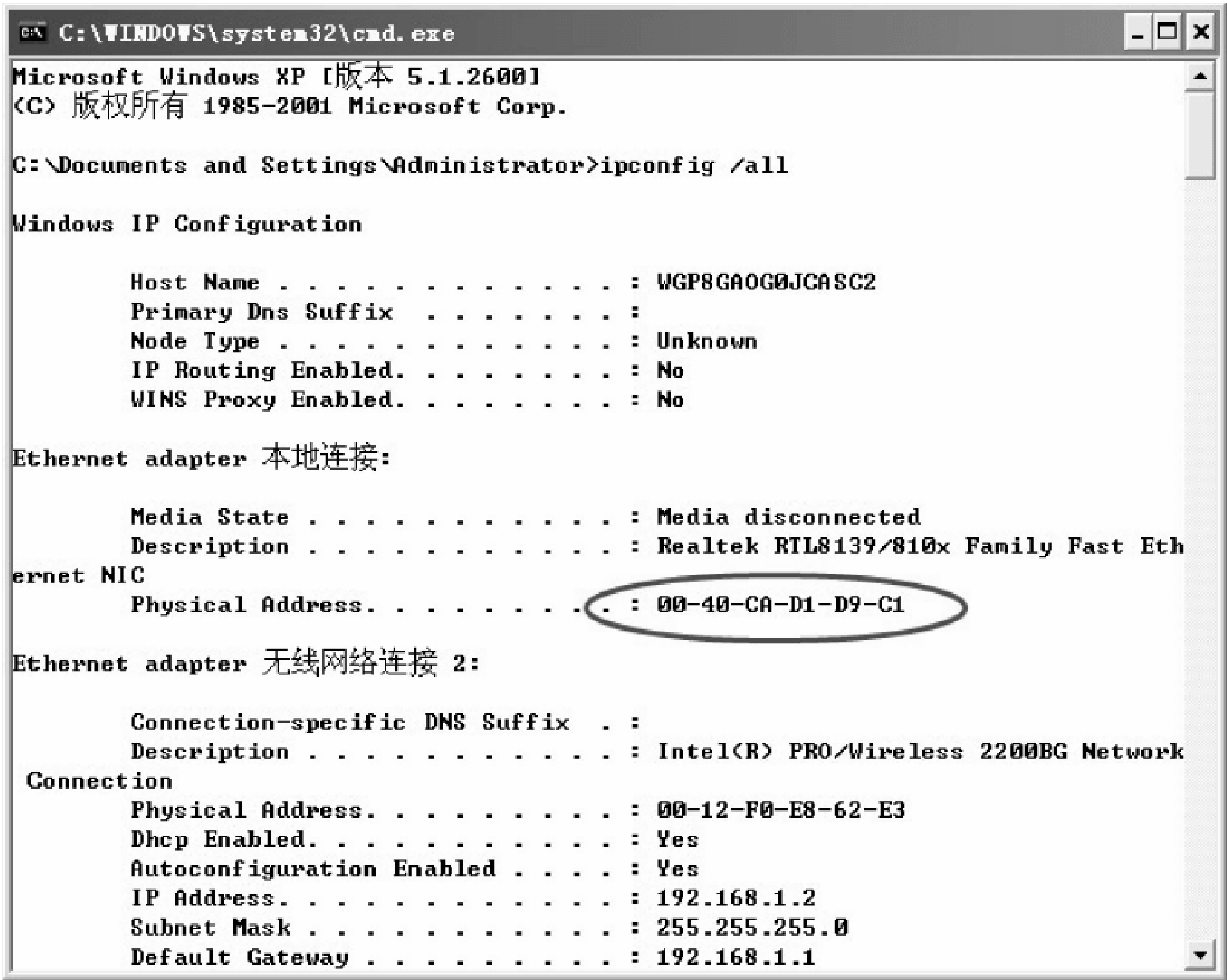



图 4-2　查看 MAC 地址

3）以太网的介质访问控制

IEEE 802.3 标准采用 CSMA/CD 协议，CSMA/CD 方式中有一个很重要的步骤，即发送站点在向网络发送帧的同时会监听网络，一旦监听到冲突就会立即停止发送，并向网络发送一个阻塞信号，通知网络已经发生了冲突，然后发送站点等待一段时间后再重发。但是如果发送站点所发送的帧的长度很短的话，那么在发送站点还未监听到冲突之前帧就已经发

送完了，此时就算监听到冲突也没有用了。因此，网络所采用的帧的长度必须保证在网络上发生冲突的情况下，在帧完全发送之前冲突能够被监听到，并及时中止发送。在采用CSMA/CD方式的网络上从冲突发生到冲突被监听到所经过的最长时间大约为51.2μs，相当于网络传输64字节数据的时间，因此可以知道以太网上帧的长度必须大于或等于64字节。

帧的长度不能大于1518字节是因为在以太网的标准中，各种协议的数据字段长度被规定为不大于1500字节。当MAC帧的数据字段小于1500字节时才被视为要传输的数据，而大于1500字节时则被视为协议代码。所以1500字节加上目的地址、源地址、数据长度、帧校验和4个字段，共18字节，总长为1518字节。因此，有效帧的长度范围为64～1518字节。以太网中MAC子层标准中规定了两个帧之间的最小间隔为9.6μs，相当于12字节数据的传输时间。因此，当一个站点要发送数据时，必须要监听到网络空闲后再等待9.6μs才能发送数据。在两个帧之间留出间隔时间是为了让刚刚接收到前一个帧的接收站点能够处理完接收缓冲区内的数据，为接收下一个帧做好准备。

4）以太网的CRC校验

循环冗余检验码CRC（Cyclic Redundancy Check）又称多项式码，它属于差错控制技术，是一种在计算机网络和数据通信中最常用的检错码。CRC通过在信息位的后面附加冗余信息，达到发现误码的目的。该种技术编解码电路简单，检错能力强，以太网中广泛应用的就是32位的CRC码。

（1）编码原理

设要发送的信息码（二进制比特序列）的长度为$k$位，CRC校验码的长度为$(n-k)$位，则编码后的总码长为$n$位。将要发送的二进制比特序列当作一个多项式$D(x)$的系数，收发双方预先约定的生成多项式为$G(x)$。CRC码在发送端编码和接收端校验时，都可以利用事先约定的生成多项式$G(x)$来得到。目前广泛使用的生成多项式主要有以下4种：

$$\text{CRC}-12 = X^{12} + X^{11} + X^{3} + X^{2} + 1$$

$$\text{CRC}-16 = X^{16} + X^{15} + X^{2} + 1 \text{（IBM 公司）}$$

$$\text{CRC}-16 = X^{16} + X^{12} + X^{5} + 1 \text{（国际电报电话咨询委员会 CCITT）}$$

$$\begin{aligned}\text{CRC}-32 = {} & X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{11} + X^{10} + X^{8} \\ & + X^{7} + X^{5} + X^{4} + X^{2} + X + 1\end{aligned}$$

（2）编码方法

将$D(x)$对应的比特序列后面填上$t$个0后作为被除数（其中$t$是$G(x)$对应的比特序列的位数减1的数，或者说，$t$是生成多项式$G(x)$的最高次幂），$G(x)$对应的比特序列作为除数，进行除法运算。注意在除法过程中所用的减法是模2减法，即没有借位的减法，也就是异或运算。当被除数逐位除完时，得到一个比除数少1位的余数即为CRC校验码，然后将它附加在要发送的信息码后面一并发往信道。接收端收到全部码字后，采用同样的方法进行验证，即将收到的码字除以$G(x)$，若余数是0，则认为码字在传输过程中没有出错。若

余数不是 0，则认为码字在传输过程中出现了差错。

(3) CRC 编码举例

假设要发送的信息位为 1011001，收发双方预先约定的生成多项式 $G(x)=X^4+X^3+1$，计算 CRC 码字。

生成多项式 $G(x)=X^4+X^3+1$，也就是 11001，因为最高次是 4，所以在信息码字(1011001)后需补 4 个 0，变为 10110010000。将 10110010000 作为被除数，11001 作为除数进行模 2 的除法运算，得到余数为 1010，即为所求的冗余位。

因此发送出去的 CRC 码字为原始码字 1011001 末尾加上冗余位 1010，即 10110011010。接收端采用同样的方法进行验证，即将收到的码字除以 11001，发现余数是 0，则认为码字在传输过程中没有出错。

(4) CRC 码的特性

CRC 码有两个重要特性，可通过下面的 $(n,k)$ 码实例来说明。

例如在(7,3)码中，要传送的信息码长度有 3 位，可分别表示十进制数据 0～7，设生成多项式 $G(x)=X^4+X^3+X^2+1$，则通过 CRC 校验计算，可得表 4-1 结果。

- 封闭性：上表中任意两个(7,3)CRC 码的对应位进行模 2 运算(异或)后得到的结果，仍然是表中 8 个码字中的一个。
- 循环性：上表中任意一个(7,3)CRC 码字循环右移一位或多位后，仍然是表中 8 个码字中的一个。

表 4-1　(7,3)CRC 码

| 信息位 | (7,3)CRC 码 |
|---|---|
| 000 | 000 0000 |
| 001 | 001 1101 |
| 010 | 010 0111 |
| 011 | 011 1010 |
| 100 | 100 1110 |
| 101 | 101 0011 |
| 110 | 110 1001 |
| 111 | 111 0100 |

使用这种冗余编码的实质在于，传输信息符号时，不使用全部编码组合，而只使用其中的一部分，这部分编码具有某种事先确定的性质(封闭性和循环性)。在接收端出现不使用的编码组合(禁用码)时，则说明在某一位或若干位中发生了错误。

因为除法运算易于用移位寄存器和模 2 加法器实现，因此循环冗余校验码的编译码过程通常采用硬件实现，而且可以达到较高的处理速度。随着集成电路工艺的发展，循环冗余码的产生和校验均有集成电路产品，发送端能够自动生成 CRC 码，接收端自动校验，速度大大提高。Ethernet 信道编码采用的是 32 位 CRC 码，它由专用的以太网系列器件来实现。

**2. 10Mb/s 以太网(标准以太网)**

开始以太网只有 10Mb/s 的吞吐量，使用的是带有冲突检测的载波侦听多路访问(CSMA/CD)的访问控制方法，这种早期的 10Mb/s 以太网称之为标准以太网。以太网可以使用粗同轴电缆、细同轴电缆、非屏蔽双绞线、屏蔽双绞线和光纤等多种传输介质进行连接，并且在 IEEE 802.3 标准中，为不同的传输介质制定了不同的物理层标准，在这些标准中前面的数字表示传输速度，单位是“Mb/s”，最后的一个数字表示单段网线长度(基准单位

是 100m)，Base 表示“基带”的意思，Broad 代表“宽带”。

IEEE 802.3 中规定为 6 种标准，分别对网络拓扑、数据速率、信号编码、最大网段长度及所使用的传输介质进行了规定，如表 4-2 所示。

**表 4-2 IEEE 802.3 中规定的 6 种标准**

| 内　　容 | 10Base5 | 10Base2 | 10Broad36 | 10Base-T | 1Base5 | 10Base-F |
|---|---|---|---|---|---|---|
| 拓扑结构 | 总线型 | 总线型 | 总线型 | 星型 | 星型 | 星型 |
| 数据速率 | 10Mb/s | 10Mb/s | 10Mb/s | 10Mb/s | 1Mb/s | 10Mb/s |
| 编码类型 | 曼彻斯特 | 曼彻斯特 | 宽带 DPSK | 曼彻斯特 | 曼彻斯特 | 曼彻斯特 |
| 最大网段长度 | 500m | 185m | 1800m | 100m | 500m | 2000m |
| 传输介质 | 50Ω 粗缆 | 50Ω 细缆 | 75Ω 同轴电缆 | UTP | UTP | 光纤 |

**3. 100Mb/s 以太网(快速以太网)**

1992 年，传输速率为 100Mb/s 的以太网问世，称之为快速以太网，或高速以太网。目前，几乎大部分的 100Mb/s 的以太网设备都与 10Mb/s 的以太网设备兼容。100Mb/s 以太网标准存在两个分别独立的标准：一个是 IEEE 802.3u 的 100Base-T；另一个是 IEEE 802.12 的 100VG-AnyLAN。前者主要由 3COM、Intel 和 Sun 等公司支持，采用的是 CSMA/CD 访问控制协议；后者主要由 HP、IBM 等公司支持，采用的是类似于令牌网的需求优先访问控制协议，支持 IEEE 802.3 帧结构。由于 100VG-AnyLAN 标准和 10Base-T 标准之间的兼容性较差，支持的厂商较少，所以没有得到广泛的应用。

快速以太网技术可以有效地保障用户在布线基础实施上的投资，它支持 3、4、5 类双绞线以及光纤的连接，能有效地利用现有的设施。快速以太网的不足其实也是以太网技术的不足，那就是快速以太网仍是基于 CSMA/CD 技术，当网络负载较重时，会造成效率的降低，当然这可以使用交换技术来弥补。100Mb/s 快速以太网标准又分为：100Base-TX、100Base-FX、100Base-T4 三个子类。

(1) 100Base-TX 是一种使用 5 类数据级无屏蔽双绞线或屏蔽双绞线的快速以太网技术。它使用两对双绞线，一对用于发送，一对用于接收数据。在传输中使用 4B/5B 编码方式，信号频率为 125MHz。符合 EIA586 的 5 类布线标准和 IBM 的 SPT 1 类布线标准。使用同 10BASE-T 相同的 RJ-45 连接器。它的最大网段长度为 100 米。它支持全双工的数据传输。

(2) 100Base-FX 是一种使用光缆的快速以太网技术，可使用单模和多模光纤(62.5μm 和 125μm)。多模光纤连接的最大距离为 550 米。单模光纤连接的最大距离为 3000 米。在传输中使用 4B/5B 编码方式，信号频率为 125MHz。它使用 MIC/FDDI 连接器、ST 连接器或 SC 连接器。它的最大网段长度为 150m、412m、2000m 或更长至 10 千米，这与所使用的光纤类型和工作模式有关，它支持全双工的数据传输。100Base-FX 特别适合于有电气干扰的环境、较大距离连接或高保密环境等情况。

（3）100Base-T4 是一种可使用 3、4、5 类无屏蔽双绞线或屏蔽双绞线的快速以太网技术。100Base-T4 使用 4 对双绞线，其中的三对用于在 33MHz 的频率上传输数据，每一对均工作于半双工模式。第四对用于 CSMA/CD 冲突检测。在传输中使用 8B/6T 编码方式，信号频率为 25MHz，符合 EIA586 结构化布线标准。它使用与 10Base-T 相同的 RJ-45 连接器，最大网段长度为 100m。

**4．1000Mb/s 以太网**

千兆以太网技术作为最新的高速以太网技术，给用户带来了提高核心网络的有效解决方案，这种解决方案的最大优点是继承了传统以太技术价格便宜的优点。千兆技术仍然是以太技术，它采用与 10Mb/s 以太网相同的帧格式、帧结构、网络协议、全/半双工工作方式、流控模式以及布线系统。由于该技术不改变传统以太网的桌面应用、操作系统，因此可与 10Mb/s 或 100Mb/s 的以太网很好地配合工作。升级到千兆以太网不必改变网络应用程序、网管部件和网络操作系统，能够最大程度地保护投资。千兆以太网的出现填补了 802.3 以太网/快速以太网标准的不足。

与传统的以太网技术相似，千兆位以太网定义了各种介质传输。目前，千兆位以太网存在两个标准，分别为 IEEE 802.3z 的 1000Base-X 标准和 IEEE 802.3ab 的 1000Base-T 标准。

1）IEEE 802.3z

IEEE 802.3z 工作组负责制定光纤（单模或多模）和同轴电缆的全双工链路标准。IEEE 802.3z 定义了基于光纤和短距离铜缆的 1000Base-X，采用 8B/10B 编码技术，信道传输速度为 1.25Gb/s，去耦后实现 1000Mb/s 传输速度。IEEE 802.3z 具有下列千兆以太网标准：

（1）1000Base-SX：只支持多模光纤，可以采用直径为 62.5μm 或 50μm 的多模光纤，工作波长为 770～860nm，传输距离为 220～550m。

（2）1000Base-LX：可以支持直径为 9μm 或 10μm 的单模光纤，工作波长范围为 1270～1355nm，传输距离为 5km 左右。

（3）1000Base-CX：采用 150Ω 屏蔽双绞线（STP），传输距离为 25m。

2）IEEE 802.3ab

IEEE 802.3ab 工作组负责制定基于 UTP 的半双工链路的千兆以太网标准，产生 IEEE 802.3ab 标准及协议。IEEE 802.3ab 定义基于 5 类 UTP 的 1000Base-T 标准，其目的是在 5 类 UTP 上以 1000Mb/s 速率传输 100m。IEEE 802.3ab 标准的意义主要有两点：

（1）保护用户在 5 类 UTP 布线系统上的投资。

（2）1000Base-T 是 100Base-T 的自然扩展，与 10Base-T、100Base-T 完全兼容。不过，在 5 类 UTP 上达到 1000Mb/s 的传输速率需要解决 5 类 UTP 的串扰和衰减问题，因此，使 IEEE 802.3ab 工作组的开发任务要比 IEEE 802.3z 复杂些。

**5. 10000Mb/s 以太网**

2002 年 6 月，正式发布了 802.3ae 10GE 标准。在物理层，802.3ae 大体分为两种类型：一种为与传统以太网连接，速率为 10Gb/s 的“LAN PHY”(局域网物理层)；另一种为连接 SDH/SONET，速率为 9.58464Gb/s 的“WAN PHY”(广域网物理层)。

在数据链路层 IEEE 802.3ae 继承了 IEEE 802.3 以太网的帧结构和帧长度，支持多层星型连接、点到点连接及其组合，充分兼容已有应用，且不影响上层应用，进而降低了升级风险。

与传统的以太网不同，IEEE 802.3ae 仅仅支持全双工方式，不再提供对单工和半双工方式的支持，不采用 CSMA/CD 机制；IEEE 802.3ae 不支持自协商，可简化故障定位，并提供广域网物理层接口。

### 4.1.5 以太网的核心设备

在计算机网络系统中，交换概念的提出改进了局域网的共享工作模式。交换(Switching)是按照通信两端传输信息的需要，用人工或设备自动完成的方法，把要传输的信息送到符合要求的相应路由上的技术的统称。广义的交换机(Switch)就是一种在通信系统中完成信息交换功能的设备，它能把用户线路、电信电路和(或)其他要互连的功能单元根据单个用户的请求连接起来。随着计算机及其互联技术的迅速发展，以太网成为了迄今为止普及率最高的短距离二层计算机网络，而以太网的核心部件就是以太网交换机。

**1. 以太网交换机的工作原理**

以太网交换机是基于以太网传输数据的网络设备，能够完成封装转发数据包的功能。作为局域网的主要连接设备，以太网交换机成为应用普及最快的网络设备之一。以太网交换机工作在数据链路层，使用 48 位的物理地址(MAC 地址)，为两点间提供“独享通路”。由于交换机采用接收、查表、转发的工作方式，交换机的各个端口分属于不同的冲突域，因此能有效提高交换机的性能和数据转发能力。如果交换机每个端口有大量数据发送，则端口会先将收到的等待发送的数据存储到寄存器中，在轮到发送时再将其发送出去。

每个交换机都有一个 MAC 地址表，MAC 地址表中记录了交换机所了解的所有站点的 MAC 地址信息(站点网卡 MAC 地址和交换机上连接这个地址的端口)。以太网交换机就是通过 MAC 地址来转发数据的，其工作原理大致可以分为下列 5 个过程。

1) 学习

交换机刚刚启动时，它的 MAC 地址表内是无任何表项的。以太网交换机了解每一端口相连设备的 MAC 地址，并将地址与相应的端口映射起来存放在交换机缓存中的 MAC 地址表中，这就是交换机的学习功能。

交换机只会学习单播数据帧的源地址，任何站点都不可能产生以广播地址或多播地址为源地址的数据帧。

2）泛洪

当接收到一个数据帧后，交换机将数据帧中的目的 MAC 地址同已建立的 MAC 地址表进行比较，以决定由哪个端口进行转发。若数据帧中的目的地址不在 MAC 地址表中，交换机则向除接收到该数据帧的端口外的其他所有端口泛洪（广播）该数据帧。

3）过滤

当交换机查看数据帧中的目的地址然后去决定怎样转发数据帧时，若发现源 MAC 地址和目的 MAC 地址处于交换机的同一个端口上，交换机会丢弃这个数据帧（过滤），因为没有必要将这个数据帧转发出去，那样只会浪费带宽。

4）转发

当交换机查看数据帧中的目的地址然后去决定怎样转发数据帧时，若发现数据帧的目的地址在 MAC 地址表中有映射，则根据 MAC 地址表转发数据帧到连接目的节点的端口而不是所有端口。

5）更新

当交换机学习到一个地址时，它将地址加入到自己的 MAC 地址表中，同时会为这个条目分配一个老化计时器，通常交换机 MAC 地址表的老化时间是 300s，即 MAC 地址在 MAC 地址表中存在的时间，当计时器到期时，交换机就会将这个条目移除。如果在老化计时器还未到期时，交换机又接收到一个来自该地址的数据帧，它将 MAC 地址重新学习到新的端口，即刷新这个计时器并重新开始计时。

**2. 以太网交换机的工作方式**

1）存储转发式

存储转发方式是计算机网络中应用最为广泛的方式。当交换机运行存储转发模式时，在转发数据帧之前必须接收整个数据帧先存储起来，检查其源地址和目标地址，然后对整个数据帧进行 CRC（循环冗余校验码）校验。如果交换机没有发现错误，它将取出数据帧的目的地址，通过查找表转换成输出端口送出数据帧。如果交换机发现数据帧中存在错误，它将丢弃这个数据帧。

由于交换机在开始转发数据之前必须接收完整个数据帧，所以存储转发方式在数据处理时延时大，这是它的不足，但是它可以对进入交换机的数据包进行错误检测，有效地改善网络性能。尤其重要的是它可以支持不同速度的端口间的转换，保持高速端口与低速端口间的协同工作。

2）直通式

直通方式的以太网交换机可以理解为在各端口间是纵横交叉的线路矩阵电话交换机。它在输入端口检测到一个数据包时，检查该包的包头，获取包的目的地址，启动内部的动态查找表转换成相应的输出端口，在输入与输出交叉处接通，把数据包直通到相应的端口，实现交换功能。

直通方式允许交换机在检查到数据帧中的目标地址时就开始转发数据。目标地址在数

据帧中占用 6 字节(这 6 字节正是目标设备的 MAC 地址),因为它不需要像存储转发那样等待接收到完整的数据帧之后再开始转发,而只需要接收到前 6 字节后就可以开始转发数据帧,所以直通式的延迟非常小、交换非常快,这是它的优点。

直通式也有它的缺点,因为数据包内容并没有被以太网交换机保存下来,所以无法检查所传送的数据包是否有误,不能提供错误检测能力。由于没有缓存,不能将具有不同速率的输入/输出端口直接接通,而且容易丢包。

随着交换机处理器速度的提升,在高性能的网络中,交换机接受和处理数据帧的延迟变得越来越小,直通式的优势也变得越来越小。存储转发模式的优势越来越明显。

3) 碎片隔离式

碎片隔离交换模式是介于前两者之间的一种解决方案,也称为碎片丢弃交换模式或自由分段模式。该模式先检查数据包的长度是否够 64 个字节,如果小于 64 字节,说明是假包,则丢弃该包;如果大于 64 字节,则发送该包。采用这种交换模式的原因是当网络发生冲突时会产生小于 64 字节的冲突碎片(Collision Fragment),冲突碎片是无效的数据帧,应该丢弃。

碎片隔离方式不提供数据校验,它有效地结合了存储转发模式和直通式的优点,数据处理速度比存储转发方式快,但比直通式慢。某些品牌的交换机如 Cisco 就提供了这种工作方式。

**3. 多层交换技术**

在计算机网络应用早期,局域网工作在共享模式下,即共享式局域网。随着各种应用对网络带宽需求的进一步提升,交换机替代了集线器和网桥,第二层交换机在网络中得到了广泛应用,局域网也由传统的共享式局域网发展为交换式局域网。

然而,局域网交换技术并没有为大规模的局域网的建设提供一个完整、系统的解决方案。随着以 Internet 为代表的互联网技术的发展,局域网在扩大自身规模的同时,开始接入互联网,以实现最大范围的数据共享和交换。在此种情况下,交换机与路由器的结合成为必然。为减少网络堵塞、优化网络结构、提高网络吞吐量、细化网络管理,多层交换技术应运而生。

目前,以太网交换机厂商根据市场需求,推出了三层甚至四层交换机。但无论如何,其核心功能仍是二层的以太网数据包交换,只是带有了一定的处理 IP 层甚至更高层数据包的能力。

## 4.2 虚拟局域网

VLAN(Virtual Local Area Network)的中文名为"虚拟局域网"。VLAN 是一种将局域网设备从逻辑上划分成一个个网段,从而实现虚拟工作组的新兴数据交换技术。这一新兴技术主要应用于交换机和路由器中,但主流应用还是在交换机之中。但又不是所有交换

机都具有此功能，只有 VLAN 协议的第三层以上交换机才具有此功能。

IEEE 于 1999 年颁布了用以标准化 VLAN 实现方案的 802.1Q 协议标准草案。VLAN 技术的出现，使得管理员根据实际应用需求，把同一物理局域网内的不同用户逻辑地划分成不同的广播域，每一个 VLAN 都包含一组有着相同需求的计算机工作站，与物理上形成的 LAN 有着相同的属性。由于它是从逻辑上划分，而不是从物理上划分，所以同一个 VLAN 内的各个工作站没有限制在同一个物理范围中，即这些工作站可以在不同物理 LAN 网段。由 VLAN 的特点可知，一个 VLAN 内部的广播和单播流量都不会转发到其他 VLAN 中，从而有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。

### 4.2.1　虚拟局域网概述

虚拟局域网(VLAN)是一组逻辑上的设备和用户，这些设备和用户并不受物理位置的限制，可以根据功能、部门及应用等因素将它们组织起来，相互之间的通信就好像它们在同一个网段中一样，由此得名虚拟局域网。VLAN 是一种比较新的技术，工作在 OSI 参考模型的第 2 层和第 3 层，一个 VLAN 就是一个广播域，VLAN 之间的通信是通过第 3 层的路由器来完成的。与传统的局域网技术相比较，VLAN 技术更加灵活，它具有以下优点。

**1. 抑制广播风暴**

限制网络上的广播，将网络划分为多个 VLAN 可减少参与广播风暴的设备数量。LAN 分段可以防止广播风暴波及整个网络。VLAN 可以提供建立防火墙的机制，防止交换网络的过量广播。使用 VLAN，可以将某个交换端口或用户赋予某一个特定的 VLAN 组，该 VLAN 组可以在一个交换网中或跨接多个交换机，在一个 VLAN 中的广播不会送到 VLAN 之外。同样，相邻的端口不会收到其他 VLAN 产生的广播。这样可以减少广播流量，释放带宽给用户应用，减少广播的产生。

**2. 安全**

增强局域网的安全性，含有敏感数据的用户组可与网络的其余部分隔离，从而降低泄露机密信息的可能性。不同 VLAN 内的报文在传输时是相互隔离的，即一个 VLAN 内的用户不能和其他 VLAN 内的用户直接通信，如果不同 VLAN 要进行通信，则需要通过路由器或三层交换机等三层设备。

**3. 成本降低，性能提高**

成本高昂的网络升级需求减少，现有带宽和上行链路的利用率更高，因此可节约成本。同时，将第二层平面网络划分为多个逻辑工作组(广播域)可以减少网络上不必要的流量并提高性能。

**4. 简化项目管理或应用管理**

VLAN 将用户和网络设备聚合到一起，以支持商业需求或地域上的需求。通过职能划分，项目管理或特殊应用的处理都变得十分方便。此外，也很容易确定升级网络服务的影响范围。

**5. 增加网络连接的灵活性**

借助 VLAN 技术,能将不同地点、不同网络、不同用户组合在一起,形成一个虚拟的网络环境,就像使用本地 LAN 一样方便、灵活、有效。VLAN 可以降低移动或变更工作站地理位置的管理费用,特别是一些业务情况有经常性变动的公司使用了 VLAN 后,这部分管理费用大大降低。

## 4.2.2 虚拟局域网的实现

从技术角度讲,实现 VLAN 的划分可依据不同的原则,一般有以下三种划分方法。

**1. 基于端口的 VLAN 划分**

这种划分是把一个或多个交换机上的几个端口划分为一个逻辑组,这是最简单、最有效的划分方法。该方法只需网络管理员对网络设备的交换端口进行重新分配即可,不用考虑该端口所连接的设备。基于端口的 VLAN 的划分是最简单最有效的 VLAN 划分方法,它按照局域网交换机端口来定义 VLAN 成员。VLAN 从逻辑上把局域网交换机的端口划分开来,从而把终端系统划分为不同的部分,各部分相对独立,在功能上模拟了传统的局域网。

基于端口的 VLAN 划分又分为在单交换机端口和多交换机端口定义 VLAN 两种情况。

1)单交换机端口定义 VLAN

许多 VLAN 厂商都利用交换机的端口来划分 VLAN 成员。被设定的端口都在同一个广播域中。如图 4-3 所示,一个交换机的 1、2、6、7、8 端口被定义为虚拟网 VLAN1,同一交换机的 3、4、5 端口组成虚拟网 VLAN2。这样做允许各端口之间的通信,并允许共享型网络的升级。但是这种划分模式将虚拟网限制在了同一台交换机上,也就是说,这种 VLAN 只支持一个交换机。

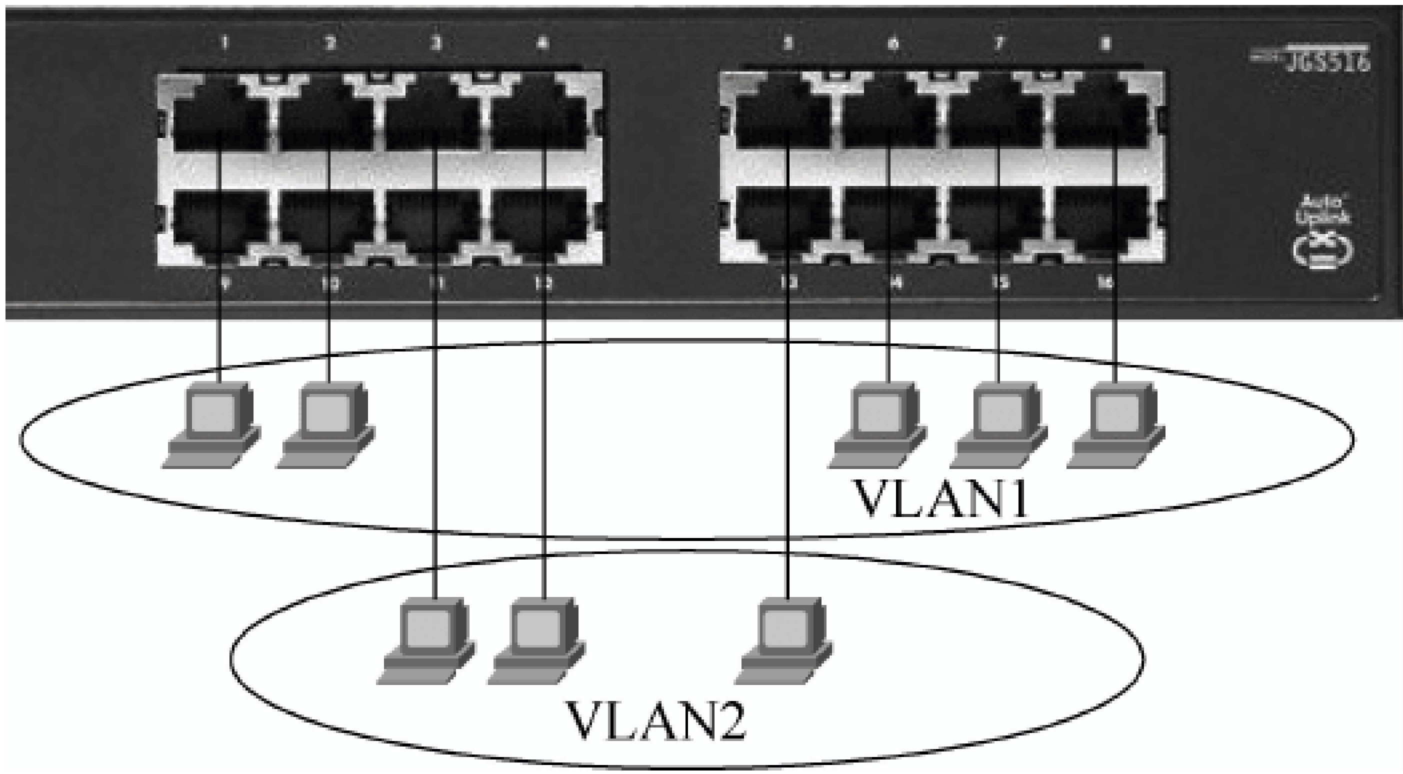



图 4-3 单交换机端口 VLAN 划分

2)多交换机端口定义 VLAN

第二代端口 VLAN 技术允许跨越多个交换机的多个不同端口划分 VLAN,不同交换机上的若干个端口可以组成同一个虚拟网。如图 4-4 所示,交换机 1 的 1、2、3 端口和交

换机 2 的 4、5、6 端口组成 VLAN1，交换机 1 的 5、6 端口和交换机 2 的 1、3 端口组成 VLAN2。

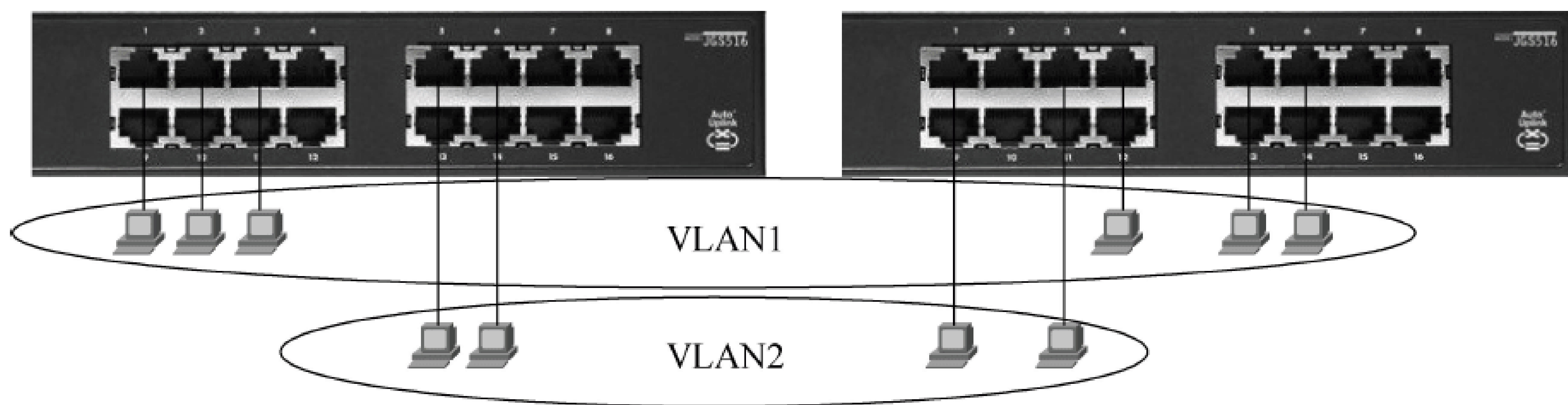



图 4-4 多交换机端口 VLAN 划分

基于交换机端口的 VLAN 划分简单、有效，其配置过程简单明了。因此，从目前来看，这种根据端口来划分 VLAN 的方式仍然是最常用的一种方式。但其缺点是当用户从一个端口移动到另一个端口时，网络管理员必须对 VLAN 成员进行重新配置。

**2. 基于 MAC 地址的 VLAN 划分**

MAC 地址其实就是指网卡的标识符，每一块网卡的 MAC 地址都是唯一且固化在网卡上的。MAC 地址由 12 位十六进制数表示，前 6 位为网卡的厂商标识（Organizationally Unique Identifier，OUI），后 6 位为网卡标识（Network Inter face Cavd，NIC）。网络管理员可按 MAC 地址把一些站点划分为一个逻辑子网。

基于 MAC 地址的 VLAN 是用终端系统的 MAC 地址定义的 VLAN。MAC 地址其实就是指网卡的标识符，每一块网卡的 MAC 地址都是唯一的。这种方法允许工作站移动到网络的其他物理网段，而自动保持原来的 VLAN 成员资格。在网络规模较小时，该方案可以说是一个好的方法，但随着网络规模的扩大，网络设备、用户的增加，则会在很大程度上加大管理的难度。

这种划分 VLAN 的方法是根据每个主机的 MAC 地址来划分，即对每个 MAC 地址的主机都配置它属于哪个组。这种划分 VLAN 方法的最大优点就是当用户物理位置移动时，即从一个交换机换到其他的交换机时，VLAN 不用重新配置，所以，可以认为这种根据 MAC 地址的划分方法是基于用户的 VLAN，这种方法的缺点是初始化时，所有的用户都必须进行配置，如果有几百个甚至上千个用户的话，配置是非常累的。而且这种划分的方法也导致了交换机执行效率的降低，因为在每一个交换机的端口都可能存在很多个 VLAN 组的成员，这样就无法限制广播包了。另外，对于使用笔记本电脑的用户来说，他们的网卡可能经常更换，这样，VLAN 就必须不停地配置。

**3. 基于路由的 VLAN 划分**

路由协议工作在网络层，相应的工作设备有路由器和路由交换机（即三层交换机）。该方式允许一个 VLAN 跨越多个交换机，或一个端口位于多个 VLAN 中。这种划分 VLAN

的方法是根据每个主机的网络层地址或协议类型(如果支持多协议)划分的,如在按 IP 地址划分的 VLAN 中,很容易实现路由,即将交换功能和路由功能融合在 VLAN 交换机中。这种方式既达到了作为 VLAN 控制广播风暴的最基本目的,又不需要外接路由器,所以它与网络层的路由毫无关系。但这种方式使得 VLAN 成员之间的通信速度不是很理想。

基于路由的 VLAN 划分方法的优点是当用户的物理位置改变时,不需要重新配置所属的 VLAN,而且可以根据协议类型来划分 VLAN,这对网络管理者来说很重要;另外,这种方法不需要附加的帧标签来识别 VLAN,这样可以减少网络的通信量。

基于路由的 VLAN 划分方法的缺点是效率低,因为检查每一个数据包的网络层地址是需要消耗处理时间的(相对于前面两种方法),一般的交换机芯片都可以自动检查网络上数据包的以太网帧头,但要让芯片能检查 IP 帧头需要更高的技术,同时也更费时。当然,这与各个厂商的实现方法有关。

就目前来说,VLAN 的划分主要采取上述第 1、3 种方式,第 2 种方式为辅助性的方案。

# 4.3 无线局域网

无线局域网(Wireless LAN, WLAN)是计算机网络与无线通信技术相结合的产物。WLAN 技术开始于 20 世纪 80 年代中期,它是随着美国联邦通信委员会(Federal Communications Commission, FCC)授权公共应用使用工业、科学和医学(Industrial Scientific Medical, ISM)频段而产生的。这一政策使各大公司和终端用户不需要获得 FCC 许可证,就可以使用该频段的无线产品,从而促进了 WLAN 技术的发展和应用。通俗点说,无线局域网就是在不采用传统电缆线的同时,提供传统有线局域网的所有功能,网络所需的基础设施不需要再埋在地下或隐藏在墙里,网络能够随着用户的需要移动或变化。无线联网方式是对有线联网方式的一种补充和扩展,它使网上的计算机具有可移动性,能快速、方便地解决以有线方式不易实现的网络联通问题。目前,WLAN 的数据传输速率已经能够达到最高 600Mb/s,传输距离可远至 20km 以上。

## 4.3.1 无线局域网的协议

无线局域网所采用的是 802.11 系列标准,它也是由 IEEE 802 标准委员会制定的。最开始推出的是 802.11,但因其传输速率比较低(2Mb/s),所以没有得到广泛应用,随后又推出了改进的 802.11b 和 802.11a。目前使用最广泛的是价格低廉、速率较高(11Mb/s)的 IEEE 802.11b 产品。而 IEEE 802.11a 虽然速率快(54Mb/s),但价格昂贵,而且与之前的 802.11b 互不兼容,因此推广有一定难度。最新公布的 IEEE 802.11g 标准除具有与 IEEE 802.11a 相似的速度外,最大的特点就是与目前已经普及的 802.11b 标准具有良好的兼容性,因此具有极大的市场潜力。

**1. IEEE 802.11**

1997年,IEEE发布了802.11协议,用于解决局域网用户的无线接入。这是无线局域网领域内的第一个国际标准。IEEE 802.11业务主要限于数据访问,传输速率最高只能达到2Mb/s。

**2. IEEE 802.11b**

1999年9月,IEEE提出了高速率协议IEEE 802.11b,在IEEE 802.11的1Mb/s和2Mb/s速率基础上增加了5.5Mb/s和11Mb/s两个新的网络速率。为了支持在有噪音的环境下能够获得较好的传输速率,IEEE 802.11b支持动态速率调节技术,在理想状态下用户以11Mb/s的速率全速运行,当用户移出理想的11Mb/s速率传输的位置或距离或者受到干扰时,可将数据传输速率自动降低为5.5Mb/s、2Mb/s或1Mb/s,而且在2Mb/s、1Mb/s速率时可向下兼容IEEE 802.11。

**3. IEEE 802.11a**

1999年,IEEE 802.11a标准制定完成。该标准工作在5GHz的频段上,避开了拥挤的2.4GHz频段,传输速率可达54Mb/s,可提供25Mb/s的无线ATM接口、10Mb/s以太网无线帧结构接口和TDD/TDMA的空中接口。

和IEEE 802.11b相比,IEEE 802.11a在使用频率的选择和数据传输速率方面具有优势,但它与IEEE 802.11b不兼容,且设备较贵,点对点连接很不经济。因此,在实际应用中人们更加青睐IEEE 802.11b。

**4. IEEE 802.11g**

2003年6月,IEEE推出最新版本的IEEE 802.11g认证标准,它是一种混合标准,拥有IEEE 802.11a的传输速率,安全性较IEEE 802.11b好,并同时兼容IEEE 802.11a和IEEE 802.11b标准。

**5. IEEE 802.11n**

为了实现高带宽、高质量的WLAN服务,使无线局域网达到以太网的性能水平,IEEE 802.11任务组N(TGn)应运而生,IEEE 802.11n标准至2009年才得到IEEE的正式批准。

在传输速率方面,802.11n可以将WLAN的传输速率由目前802.11a及802.11g提供的54Mb/s,提高到300Mb/s甚至高达600Mb/s。在覆盖范围方面,802.11n采用智能天线技术,通过多组独立天线组成的天线阵列,可以动态调整波束,保证让WLAN用户接收到稳定的信号,并可以减少其他信号的干扰。因此其覆盖范围可以扩大到好几平方公里,使WLAN移动性极大提高。在兼容性方面,802.11n采用了一种软件无线电技术,它是一个完全可编程的硬件平台,使得不同系统的基站和终端都可以通过这一平台的不同软件实现互通和兼容,这使得WLAN的兼容性得到极大改善。这意味着WLAN将不但能实现802.11n向前后兼容,而且可以实现WLAN与无线广域网络的结合,比如3G。

Wi-Fi是致力于推进IEEE 802.11标准的联盟。一般Wi-Fi用来特指IEEE 802.11b标准,也常被用作IEEE 802.11标准系列的别称。IEEE 802.11标准系列及指标如表4-3所示。

表 4-3 IEEE 802.11 标准

| 标　　准 | 工 作 频 带 | 带　　宽 | 传 输 距 离 |
|---|---|---|---|
| IEEE 802.11 | 2.4GHz | 1～2Mb/s | 100m |
| IEEE 802.11b | 2.4GHz | 11Mb/s | 100～400m |
| IEEE 802.11a | 5GHz | 54Mb/s | 20～50m |
| IEEE 802.11g | 2.4GHz | 36Mb/s(最高 54Mb/s) | 100～400m |
| IEEE 802.11n | 2.4/5GHz | 300Mb/s(甚至 600Mb/s) | 十几千米 |

## 4.3.2 无线局域网的组成

与有线网络相比，WLAN 具有安装便捷灵活、传输速率高、覆盖范围广、经济节约、易于扩展、支持移动等优点。无线局域网由无线网卡、无线接入点(Access Point，AP)、计算机和有关设备组成。一个典型的无线局域网如图 4-5 所示。

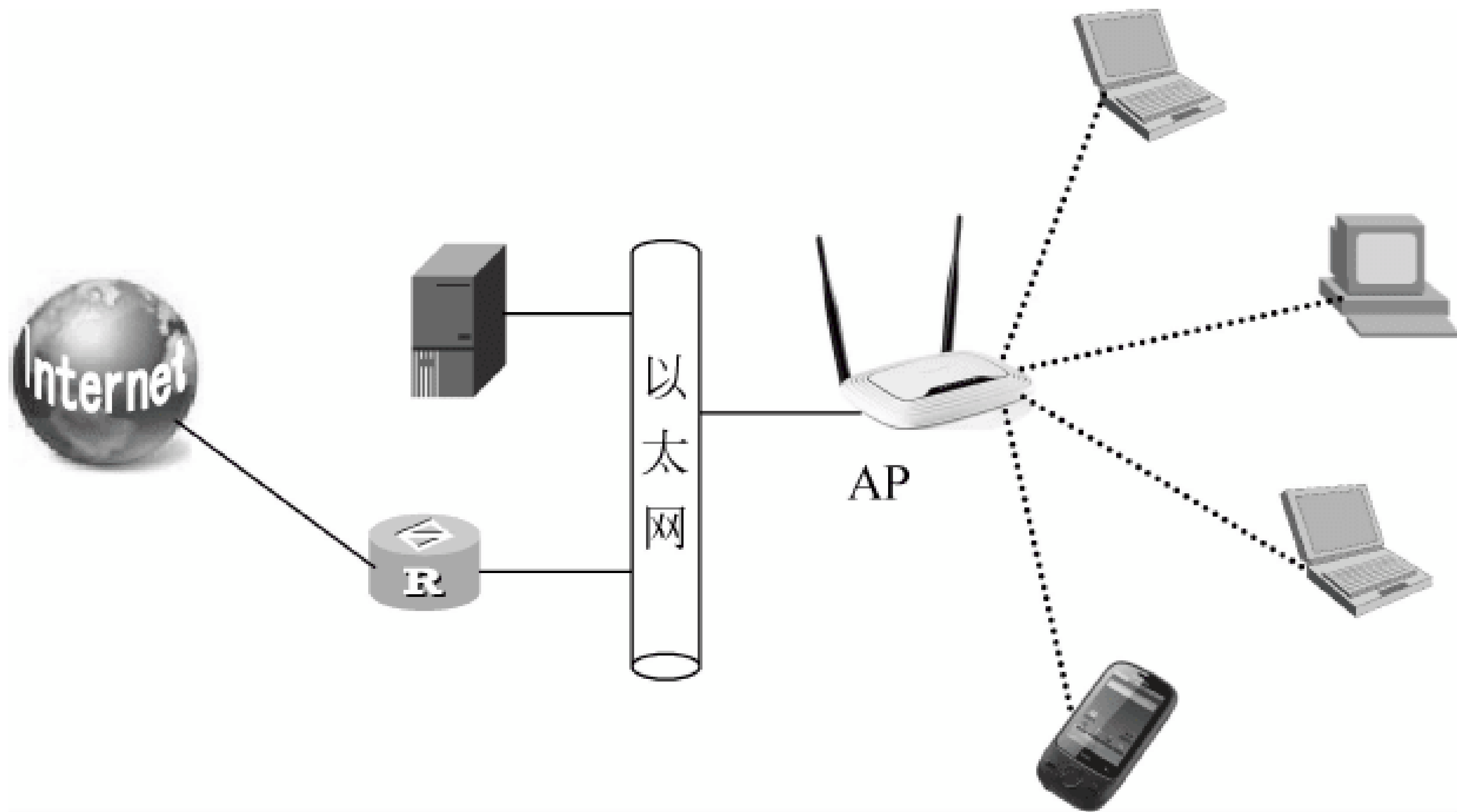



图 4-5 典型无线局域网示意图

IEEE 802.11 定义了两种类型的设备：无线站和无线接入点 AP。无线站通常是一台计算机加上一块无线网络接口卡构成，无线接入点的作用是提供无线和有线网络之间的桥接。一个无线接入点通常由一个无线输出口和一个有线的网络接口构成，桥接软件符合 IEEE 802.1d 桥接协议。接入点就像是无线网络的一个无线基站，将多个无线的接入站聚合到有线的网络上。

## 4.3.3 无线个域网 WPAN

### 1. 蓝牙

蓝牙(Bluetooth)技术是一种支持点对点、点对多点的语音、数据业务的短距离(一般在 10m 内)无线通信技术。蓝牙的创始人是瑞典爱立信公司，爱立信早在 1994 年就已进行研发。1997 年，爱立信与其他设备生产商联系，并激发了他们对该项技术的浓厚兴趣。1998 年 2 月，5 个跨国大公司，包括爱立信、诺基亚、IBM、东芝及 Intel 组成了一个特殊兴趣小组

(Special Interest Group,SIG),他们共同的目标是建立一个全球性的小范围无线通信技术,即现在的蓝牙。

蓝牙工作在全球通用的 2.4GHz ISM(即工业、科学、医学)频段,与其他工作在相同频段的系统相比,它采用分散式网络结构以及快跳频和短包技术,使蓝牙系统具有较高的抗干扰能力并很容易穿透障碍物,实现全方位的语音与数据传输。蓝牙的数据速率为 1Mb/s,采用时分双工传输方案实现全双工传输,使用 IEEE 802.15 协议。

利用 Bluetooth 技术能够有效地简化移动通信终端设备之间的通信,也能够成功地简化设备与 Internet 之间的通信,从而使数据传输变得更加迅速高效,为无线通信拓宽道路。通过使用 Bluetooth 技术产品,人们可以免除居家办公电缆缠绕的苦恼。鼠标、键盘、打印机、膝上型计算机、耳机和扬声器等均可以在 PC 环境中无线使用。此外,通过在移动设备和家用 PC 之间同步联系人和日历信息,用户可以随时随地存取最新的信息。

Bluetooth 设备不仅可以使居家办公更加轻松,用户可以在 10m 以内无线控制存储在 PC 或其他智能设备上的音频文件。Bluetooth 技术还可以用在适配器中,允许人们从相机、手机、膝上型计算机向电视发送照片等。

**2. HomeRF**

HomeRF 工作组于 1997 年成立,其主要工作任务是为家庭用户建立具有互操作性的话音和数据通信网。RF 是 Radio Frequency 的缩写,表示可以辐射到空间的电磁频率,频率范围从 300kHz～30GHz 之间。HomeRF 无线标准是由 HomeRF 工作组开发的开放性行业标准,集成了语音和数据传送技术,目的是在家庭范围内,使计算机与其他电子设备之间实现无线通信。

HomeRF 由微软、英特尔、惠普、摩托罗拉和康柏等公司提出,使用开放的 2.4GHz 频段,采用跳频扩频技术,跳频速率为 50 跳/秒,共有 75 个宽带为 1MHz 的跳频信道。HomeRF 基于共享无线接入协议(Shared Wireless Access Protocol,SWAP)。SWAP 使用 TDMA+CSMA/CA 方式,适合语音和数据业务。在进行语音通信时,采用数字增强型无绳通信标准(使用 TDMA 时分多址技术);在进行数据通信时,则采用 IEEE 802.11 的 CSMA/CA,CSMA/CA 适合于传送高速分组数据。

HomeRF 是对现有无线通信标准的综合和改进,它的优点是安全可靠,成本低廉,简单易行,不受墙壁和楼层的影响,无线电干扰影响小,支持流媒体。但是,该标准与 802.11b 不兼容,并占据了与 802.11b 和 Bluetooth 相同的 2.4GHz 频率段,所以在应用范围上会有很大的局限性,更多的是在家庭网络中使用。

**3. IrDA**

红外线数据标准协会(Infrared Data Association,IrDA)成立于 1993 年,是一个独立的非盈利性的组织,致力于建立通用的、低功率电源的、半双工红外串行数据互联标准、支持近距离、点到点、设备适应性广的用户模式。目前广泛采用的无线点对点通信技术 IrDA(红外连接技术)就是由该组织制定的一种无线协议,IrDA 建立该标准是在各种设备之间较容易

地进行低成本红外通信的关键。

红外通信利用红外技术实现两点间的近距离通信和信息转发。它一般由红外发射系统和接收系统两部分组成。发射系统对一个红外辐射源进行调制后发射红外信号,接收系统用光学装置和红外探测器进行接收。现行的 IrDA 传输速率为 16Mb/s,接收角度也由传统的 30°扩展到 120°。

IrDA 技术的主要优点是无需专门申请特定频率的使用执照,这一点在当前频率资源匮乏、频道使用费用增加的背景下是非常重要的;具有移动通信设备所必需的体积小、功率低的优点;相应的硬件及软件技术都已经比较成熟;在成本上,红外 LED 及接收器等组件较一般 RF 组件便宜很多。

IrDA 技术的缺点是 IrDA 是一种视距传输技术,在两个具有 IrDA 端口的设备之间传输数据时,中间不能有阻挡物,这在两个设备之间是比较容易实现的,但在多个电子设备间就必须彼此调整位置和角度等;另外,IrDA 设备的核心部件——红外线 LED 不是一种十分耐用的器件,对于不经常使用的扫描仪、数码相机等设备虽然游刃有余,但如果经常用装配 IrDA 端口的手机上网,可能很快就不堪重负了。

由于技术较成熟和成本较低的原因,IrDA 目前还具有一定的市场,但由于速度、距离和视距传输等限制,使得 IrDA 终究很难成为无线局域网的标准。

## 4.4 局域网组网实例

### 4.4.1 小型企业局域网

某些小型企业规模不大,只有几台(或者十几台,最多几十台)计算机和一台服务器。这样的小型企业在组建网络时可以利用一条 ADSL 线路接入 Internet,使多台计算机可以同时上网,并且还可以实现文件共享、打印机共享等。

接法:Internet-ADSL Modem-路由器-交换机-PC。

设置:先确定路由器的 IP 地址,然后在 PC 里设置 TCP/IP 协议。设置时要注意:要将 PC 和路由器的 IP 地址设置成同一网段(比如路由器的 IP 地址是 192.168.20.1,那么小型局域网的网段地址就要配置在 192.168.20.2~192.168.20.254 之间),同时将 PC 的网关配置成 192.168.20.1。

具体做法是:将计算机、服务器与一台交换机(8~16 口)相连,再通过交换机与带路由功能的 ADSL Modem 相连接,最后接入 Internet。

小型企业局域网的拓扑结构如图 4-6 所示。

### 4.4.2 中型企业局域网

一般,中型商务企业需要企业网(Intranet)、企业信息系统、共享打印机、共享 Internet 接入。在组建中型企业局域网时,要考虑下面几个方面的问题。

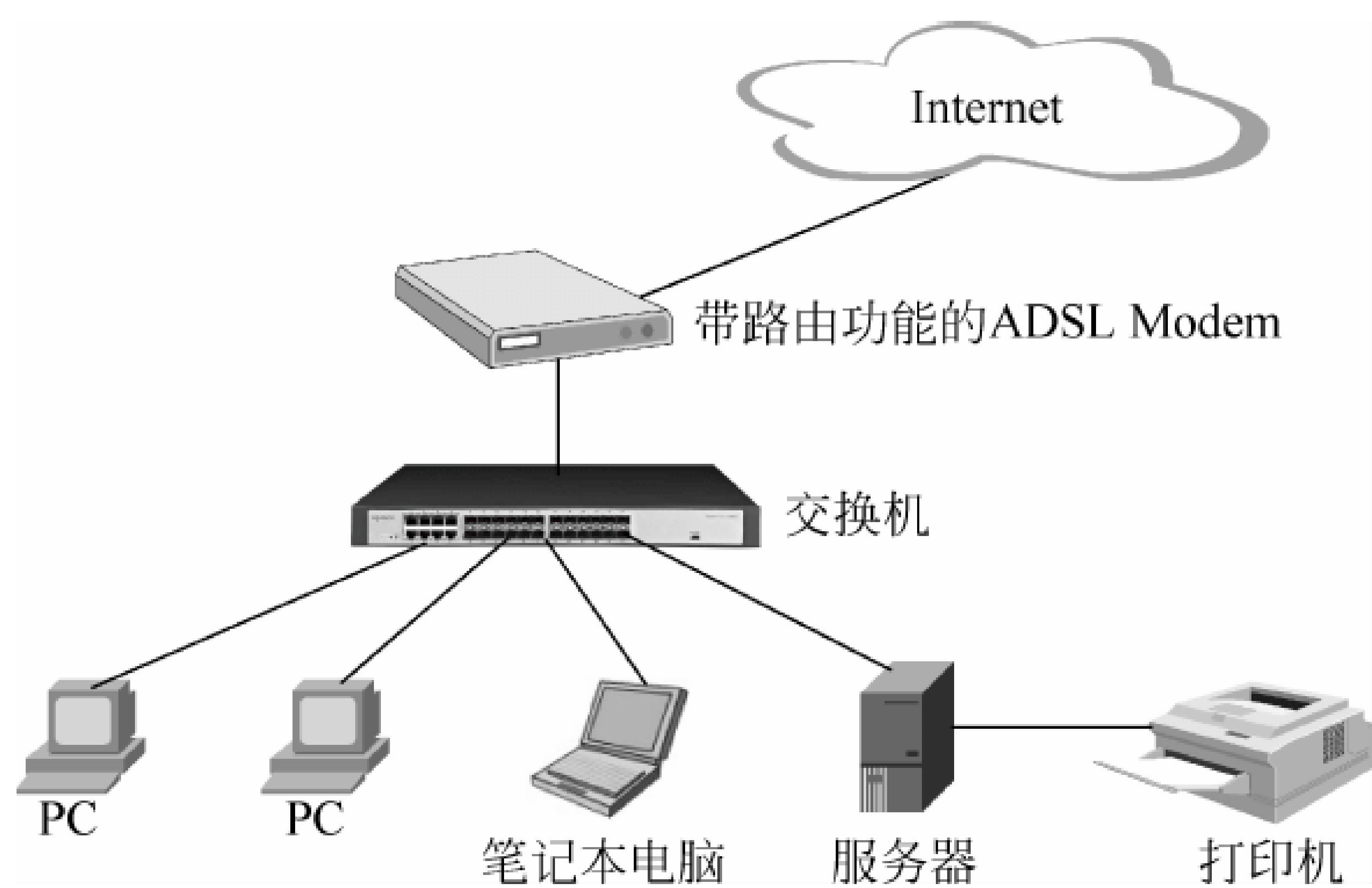



图 4-6　小型企业局域网的拓扑结构

（1）中型商务企业网应当拥有一个稳定的网络平台，接入这个系统的设备一般采用 100Mb/s 全双工交换机、服务器和客户机。

（2）需合理地划分 VLAN，这样可以有效地控制网络广播，减轻网络传输的负担，通过交换机的公共端口，提供不同 VLAN 之间的高效通信。

（3）通过授权对安全隔离加以控制。

（4）要考虑接入 Internet 和远程用户接入。

中型企业局域网的拓扑结构如图 4-7 所示。

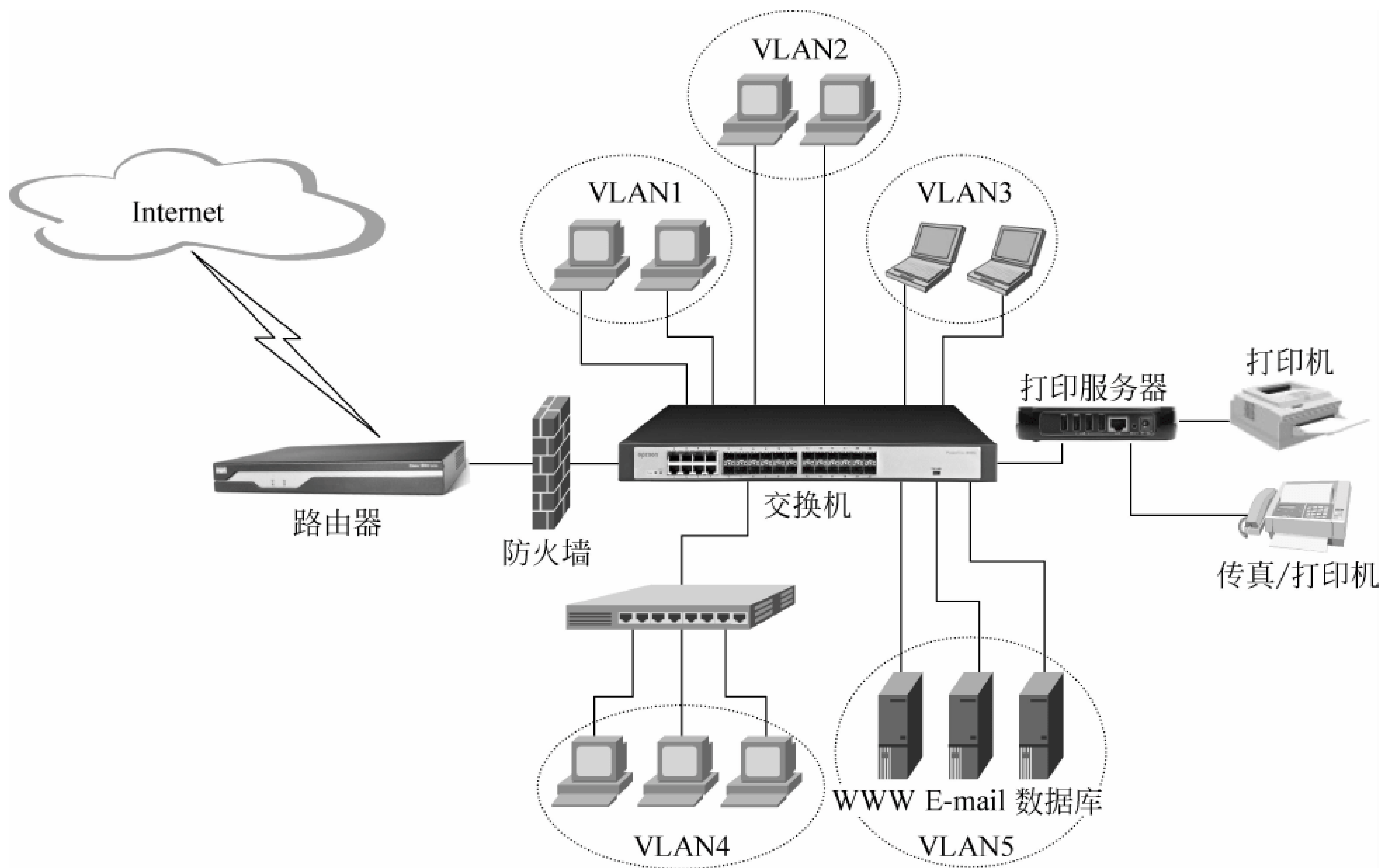



图 4-7　中型企业局域网的拓扑结构

### 4.4.3 学生宿舍无线局域网

一般大学的学生宿舍有4～8名学生，因为考虑携带的方便性，不少学生更喜欢使用笔记本电脑。目前的笔记本电脑都自带无线网卡，因此在学生宿舍组建无线网络更受欢迎。

学生宿舍组建无线局域网，要看各校宿舍的布线情况。有些新建的宿舍，每个学生均设计了信息点，每层楼都设有接入层交换机，学生上网不需要再购买交换机，直接接入信息点即可。大部分宿舍只设计了一个信息点，如果同一个宿舍的学生共享接入校园网，实现无线上网，可以采用“交换机＋无线AP”方式无线上网，也可以采用无线路由器方式无线上网，通常以使用无线路由器的方式居多。

无线路由器可以理解为将单纯性无线AP和宽带路由器合二为一的扩展型设备，它不仅具备单纯性无线AP的所有功能，如支持DHCP客户端、支持VPN、防火墙、支持WEP加密等，而且还包括了网络地址转换(Network Address Translation，NAT)功能，可支持局域网用户的网络连接共享，可实现家庭无线网络中的Internet连接共享，实现ADSL的无线共享接入。

无线路由器内部置有简单的虚拟拨号软件，可以存储用户名和密码拨号上网，可以实现为拨号接入Internet的ADSL提供自动拨号功能。此外，无线路由器一般还具备相对更完善的安全防护功能。通常的无线路由器可以看作是一个4LAN口的路由器＋无线发射端的组合，因此在条件允许的情况下，可以使一部分已经有网卡的普通台式机采用有线连接的方式。而对于不是很方便连接网线，或者是已经购买了无线网卡，或者拥有笔记本电脑的同学，就可以直接通过无线方式上网。

学生宿舍无线局域网的拓扑结构如图4-8所示。

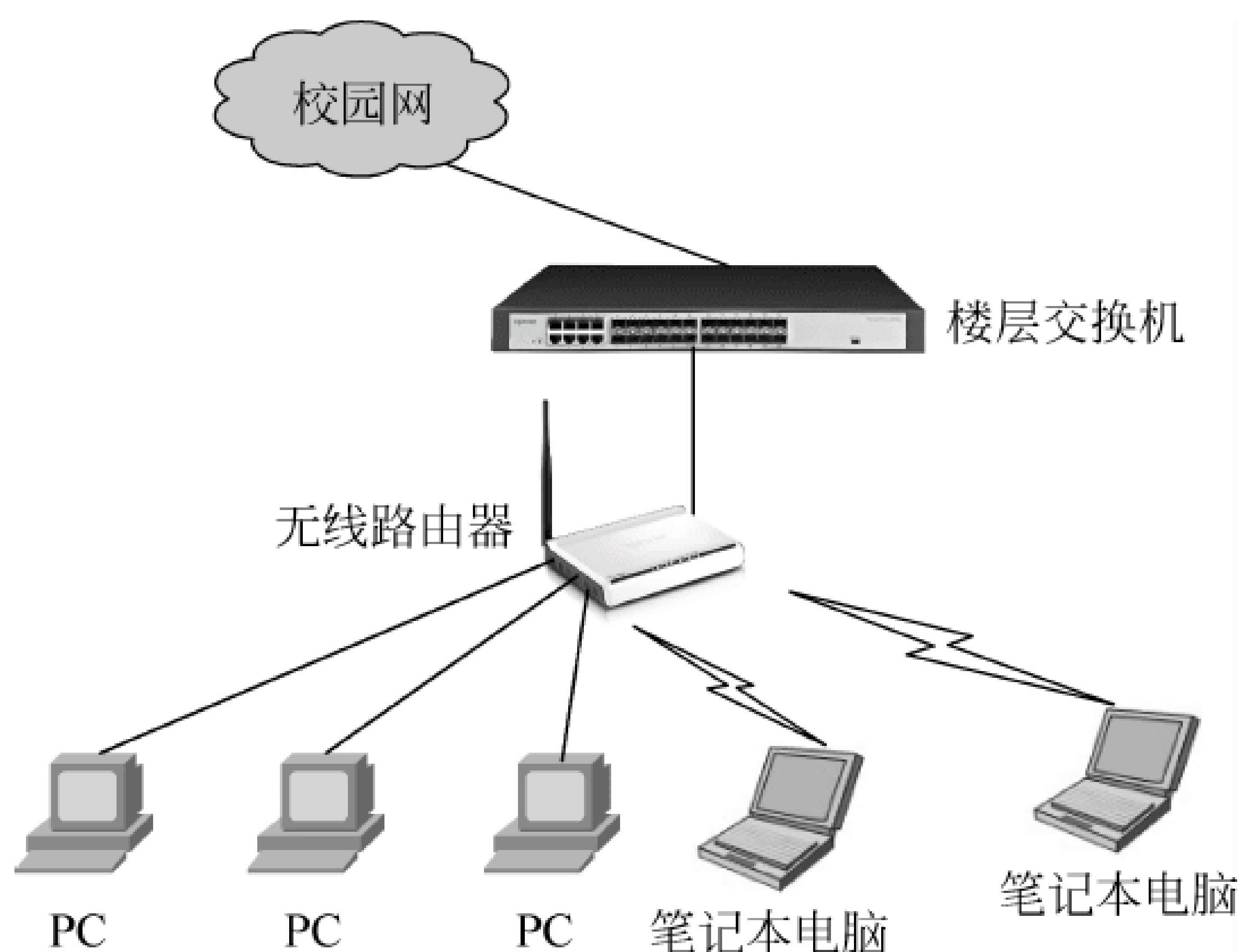



图4-8 学生宿舍无线局域网的拓扑结构

# 实验 1　网络通信线的制作

**1. 实验目标**

(1) 了解有关双绞线的基本知识。

(2) 掌握直通网线和交叉网线的制作方法和使用环境。

(3) 熟练使用压线钳、测线仪等工具制作网线。

**2. 实验准备**

双绞线、RJ-45 水晶头、压线钳、测线仪。

**3. 实验内容**

1) 双绞线的基本知识

双绞线(Twisted Pair)是局域网布线中最常用到的一种传输介质,尤其在星型网络拓扑中,双绞线是必不可少的布线材料。双绞线电缆由一对或一对以上相互扭绞在一起并相互绝缘的铜导线组成,每根铜导线的绝缘层上分别涂有不同的颜色以示区别,两条线缠绕在一起是为了减少线间的电磁干扰。

双绞线按照有无屏蔽层可分为以下两大类(如图 4-9 和图 4-10 所示)。

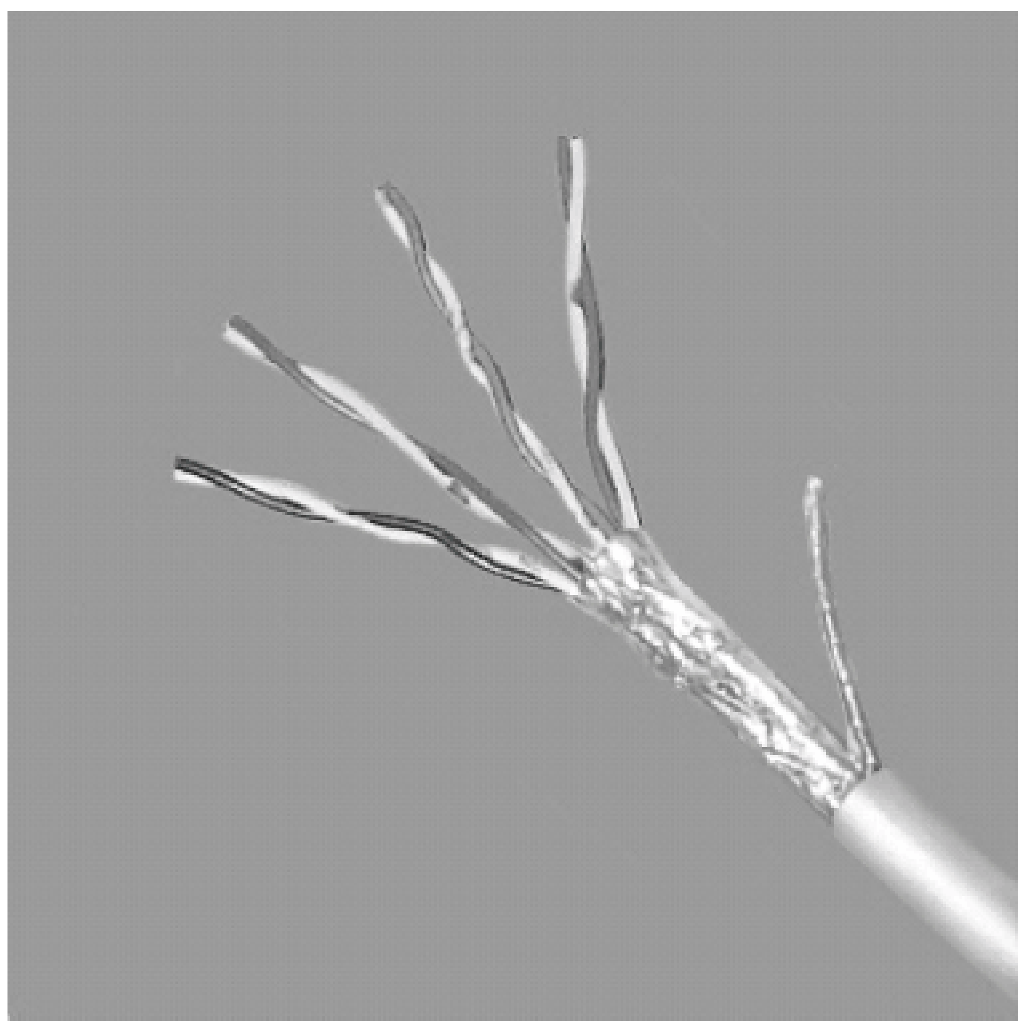


图 4-9　屏蔽双绞线(STP)



图 4-10　非屏蔽双绞线(UTP)

屏蔽双绞线(STP):金属材料包裹,减小辐射,防止信息被窃听;具有较高的数据传输速率;价格较高;安装较复杂。

非屏蔽双绞线(UTP):无金属屏蔽材料,价格相对便宜,组网灵活。

双绞线按照单位长度内的绞环数,可分为以下几个主要类别,如表 4-4 所示。

在今天的局域网布线中,使用最多的是 5 类和超 5 类 UTP。5 类 UTP 规定有 4 对(8 根)信号线,在 10/100Mb/s 以太网中,1 到 8 号线中只用了 1、2、3、6 号线,其余都是未定义的(在 1000Mb/s 以太网中使用),所以在做 10/100Mb/s 网线时,通常只需考虑 1、2、3、6 号

线的接法，剩余的线随便怎么排都没有关系（不接也可以）。EIA/TIA 568A 和 EIA/TIA 568B 的连线标准如表 4-5 所示。

**表 4-4 常见双绞线的类别**

| 类 别 | 主 要 应 用 |
|---|---|
| 3 类 | 用于以太网（10Mb/s），早期网络中重要的传输介质 |
| 4 类 | 标准推出比 3 类晚，传输性能没提高多少，较少使用 |
| 5 类 | 价廉质优，成为快速以太网（100Mb/s）的首选传输介质，最常使用 |
| 超 5 类 | 用于千兆位以太网（1000Mb/s） |
| 6 类 | 用于万兆位以太网（10Gb/s） |

**表 4-5 EIA/TIA 568A 和 EIA/TIA 568B 连线标准**

| EIA/TIA 568A 标准 | | | EIA/TIA 568B 标准 | | |
|---|---|---|---|---|---|
| 引脚顺序 | 信号定义 | 线对颜色 | 引脚顺序 | 信号定义 | 线对颜色 |
| 1 | Tx＋（传输） | 白绿 | 1 | Tx＋（传输） | 白橙 |
| 2 | Tx－（传输） | 绿 | 2 | Tx－（传输） | 橙 |
| 3 | Rx＋（接收） | 白橙 | 3 | Rx＋（接收） | 白绿 |
| 4 | 保留使用 | 蓝 | 4 | 保留使用 | 蓝 |
| 5 | 保留使用 | 白蓝 | 5 | 保留使用 | 白蓝 |
| 6 | Rx－（接收） | 橙 | 6 | Rx－（接收） | 绿 |
| 7 | 保留使用 | 白棕 | 7 | 保留使用 | 白棕 |
| 8 | 保留使用 | 棕 | 8 | 保留使用 | 棕 |

直通线：网线的两端都采用 568A 标准线序，或者都采用 568B 标准线序，只要两端相同就可以（通常为 568B 标准）。当计算机（网卡）和 Hub 或交换机等网络设备相连时，需要使用直通线。另外，直通线还用于一个 Hub 的普通口与另一个 Hub 的级联口连接等情况。

交叉线：网线的一端采用 568A 标准，另一端采用 568B 标准。当计算机（网卡）和计算机（网卡）相连时，需要使用交叉线。另外，交叉线还用于 Hub 与 Hub 间通过普通口连接，以及计算机直接连入路由器的以太网端口等情况。

**【注意】** 目前由于许多交换机和路由器都能自动识别线序，所以它们之间的连接在许多时候使用直通线和交叉线都可以。

2）制作步骤

制作双绞线需要的工具有双绞线、RJ-45 水晶头（图 4-11）、压线钳（图 4-12）和测线仪（图 4-13）。

（1）“剥”。将待剥皮的双绞线线头置于钳头的刃口中，线头留出约 2cm 的距离，用手适度捏紧两钳柄的同时慢慢旋转双绞线，让刃口划开双绞线的保护绝缘皮，轻轻一松绝缘皮便与线芯脱开，取出线头可看到两两缠绕在一起的共 8 根线芯。


图 4-11　水晶头

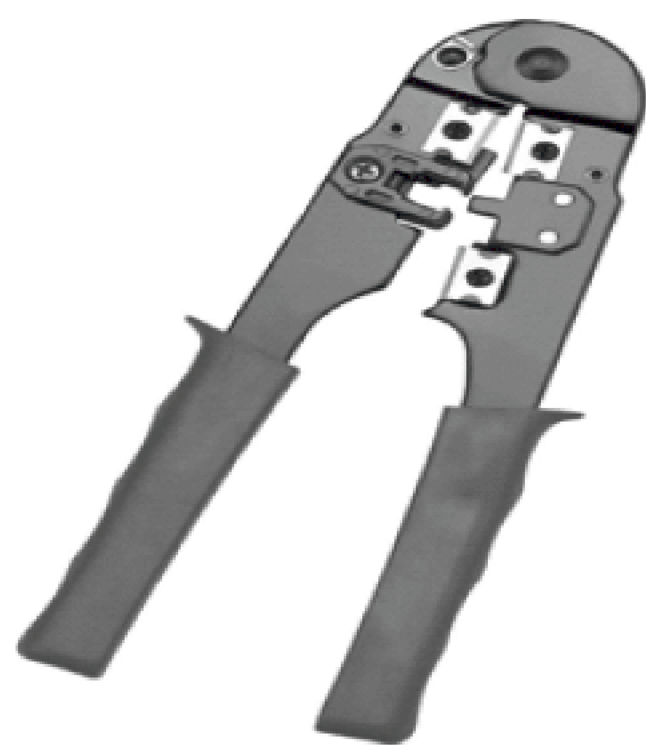

图 4-12　压线钳


图 4-13　测线仪

(2)“理”。双绞线由 8 根有色导线两两绞合而成,将 8 根线芯分开并尽量将每根线拉直,再按照 EIA/TIA 568A(或 EIA/TIA 568B)标准平行排列整齐,整理完毕后用压线钳的剪线刀口将 8 根线的前端剪整齐。

(3)“插”。将 RJ-45 连接头(水晶头)的引脚(簧片)一侧向上,将排好顺序的 8 根线芯平行插入水晶头内的线槽内,导线的顶端应插入线槽的顶端,尽量插到底。

(4)“压”。确认所有导线都到位后,将水晶头插入压线钳的压线口,用力紧握手柄压下压线钳,将水晶头的簧片插入到 8 根双绞线中。

以上方法仅制作完了双绞线的一端,按同样的方法把另一端也做好。

3) 测试

在双绞线制作好之后,还需要使用测线仪进行检测。把做好的双绞线一端的 RJ-45 连接头插入测线仪的发送端,另一端插入测线仪的接收端。开启测线仪电源开关,观察测线仪的信号指示灯会依次闪烁。如果是直通线,则指示灯闪烁的顺序为 1-1,2-2,3-3,4-4,5-5,6-6,7-7,8-8。如果是交叉线,则指示灯闪烁的顺序为 1-3,2-6,3-1,4-4,5-5,6-2,7-7,8-8。由此可以判定该双绞线制作成功,可以投入使用。如果有一个或一个以上的灯不亮,则说明 RJ-45 连接头的簧片没有全部接触到双绞线的线芯,需要重新制作。

# 实验 2　交换机的配置与管理

**1. 实验目标**

(1) 了解交换机的基本常识。

(2) 掌握交换机的基本配置命令。

**2. 实验准备**

Cisco Catalyst 2950 交换机一台,PC 一台。

**3. 实验内容**

1) 交换机的基本常识

交换机有很多种品牌和型号,各个不同型号的交换机的功能和使用范围差别很大。市

面上常见的交换机品牌有思科交换机、华为交换机、锐捷交换机等。美国的思科系统公司(Cisco System,Inc.)是全球领先的互联网设备供应商,目前互联网上近80%的信息流量经由思科系统公司的产品传递。据统计,截至2011年第一季度,思科交换机在全球的市场份额占68.5%。思科的交换机产品以“Catalyst”为商标,包含1900、2800、2900、3500、4000、5000、5500、6000、8500等十多个系列。总的来说,这些交换机可以分为两类,一类是固定配置交换机,包括3500及以下的大部分型号,此类交换机除了有限的软件升级之外,不能扩展;另一类是模块化交换机,主要指4000及以上的型号,网络设计者可以根据网络需求,选择不同数目和型号的接口板、电源模块及相应的软件。

交换机在初始启动时,系统的启动例程会初始化交换机,初始启动会利用默认设置来配置参数。接通电源后,交换机前面板指示灯的不同闪烁状态用于监控系统的活动和性能。这些指示灯称为发光二极管(Light Emitting Diode,LED),包括:

(1) 系统指示灯(SYSTEM)

SYSTEM指示灯显示系统是否已经接通电源并且正常工作。指示灯状态如表4-6所示。

**表4-6 SYSTEM指示灯状态**

| 指示灯颜色 | 系统状态 |
| --- | --- |
| 关闭 | 系统未加电 |
| 绿色 | 系统运行正常 |
| 黄色 | 系统加电但运行不正常 |

(2) 远程电源供应指示灯(Remote Power Supply,RPS)

RPS指示灯表明交换机的RPS状态,显示交换机是否有远程电源供电。指示灯状态如表4-7所示。

**表4-7 RPS指示灯状态**

| 指示灯颜色 | RPS状态 |
| --- | --- |
| 关闭 | RPS关闭或未安装 |
| 持续绿色 | RPS已连接并可用 |
| 闪烁绿色 | RPS正在支持堆叠(Stack)中的另一台交换机 |
| 持续黄色 | RPS已连接但动作不正常 |
| 闪烁黄色 | 交换机内部电源出现故障,正在使用RPS |

(3) 端口模式指示灯

端口模式指示灯显示模式(MODE)按钮的当前状态。各种模式用于决定如何对端口状态指示灯进行解释。如果要选择或改变端口模式,连续的按压Mode按钮直到Mode LED指示在所需的模式。端口状态指示灯能代表多种含义,取决于Mode LED的当前值。Mode按钮有三种状态。

STAT(状态,States):显示端口状态,这个是缺省模式。

UTL(利用率,Utilization):交换机利用率,显示目前该端口被交换机使用的带宽。

FDUP(全双工,Full Duplex):端口双工模式,可用是全双工或半双工。

如果交换机的状态灯为闪烁的黄色,一般表明在某一个端口、模块或者交换机有硬件故障;如果端口或者模块状态不正常,状态灯也为闪烁的黄色。

(4) 端口状态指示灯

交换机的每一个端口都有一个指示灯,称为端口状态指示灯(Port States LED)。这些灯显示交换机或者某单个端口的状态,不同端口模式下,端口状态指示灯表示不同的含义。详情如表4-8～表4-11所示。

**表4-8　缺省模式(STAT)下端口指示灯状态**

| 指示灯颜色 | 端口状态 |
|---|---|
| 关闭 | RPS关闭或未安装 |
| 持续绿色 | RPS已连接并可用 |
| 闪烁绿色 | RPS正在支持堆叠(Stack)中的另一台交换机 |
| 持续黄色 | RPS已连接但动作不正常 |
| 闪烁黄色 | 交换机内部电源出现故障,正在使用RPS |

**表4-9　UTIL模式下端口指示灯状态**

| 指示灯颜色 | 端口状态 |
|---|---|
| 绿色 | 当前的背板利用率 |
| 黄色 | 最大的背板利用率 |
| 绿色和黄色 | 如果所有的LED都是绿色,交换机当前的带宽使用率达到了总带宽的50%或更高;随着带宽使用率的下降,部分LED变为黄色 |

**表4-10　DUPLX模式下端口指示灯状态**

| 指示灯颜色 | 端口状态 |
|---|---|
| 关闭 | 半双工 |
| 绿色 | 全双工 |

**表4-11　SPEED模式下端口指示灯状态**

| 指示灯颜色 | 端口状态 |
|---|---|
| 关闭 | 端口运行在10Mb/s |
| 绿色 | 端口运行在100Mb/s |

在电源线连接好之后,交换机会启动一系列称为加电自测试(Power-On Self Test,POST)的测试,用于检测交换机是否工作正常。系统指示灯(System LED)会显示POST成功与否。如果交换机已经加电,系统指示灯是灭的,说明POST正在进行。如果系统指示灯变为绿色,说明POST已经成功。如果系统指示灯为黄色,则POST失败。POST失败是一个致命的错误,如果POST检测失败,交换机就不能可靠的工作。

端口状态指示灯(Port States LED)也会在POST过程中有所变化。在交换机发现网络拓扑结构并搜索环路时,端口状态指示灯会变为黄色并持续大约30s。如果端口状态指

示灯变成绿色，说明交换机的一个端口已经和目标(例如一台计算机)成功建立连接。如果端口指示灯不亮，说明交换机确定没有连接到端口的设备。

2) 交换机的基本命令模式

交换机有几种命令模式，在任何给定时间上适用于用户的命令依据当前用户所处的模式而定。在系统提示符下输入一个问号(?)能帮助获得可用于每一个命令模式的一个命令列表。

缺省模式是用户 EXEC 模式，可以通过以“>”号结尾的提示符加以识别。在用户 EXEC 模式中可以使用的命令是有限的，仅限于修改终端设置，完成基本测试和显示系统信息的命令，不能对交换机进行配置。

通过 enable 命令可以从用户 EXEC 模式切换到特权 EXEC 模式。特权 EXEC 模式通过以“#”号结尾的提示符加以识别，能对交换机进行各种配置。特权 EXEC 模式中的命令集包括在用户 EXEC 模式中允许使用的命令，另外还有 configure terminal、configure memory、configure network 命令，通过这些命令可以进入其他命令模式。由于这些模式是用于配置交换机的，所以需要密码才能够进入特权 EXEC 模式，以防止非授权的使用。如果系统管理员设置了密码，在进入特权 EXEC 模式之前会提示用户输入密码。密码的内容不会显示在屏幕上，并且密码是区分大小写的。

3) 交换机的初始配置

通过将超级终端连接到交换机的控制台端口，使用不同的 show 命令可以收集交换机当前的配置信息。

(1) 检验交换机的缺省配置：Switch# **show run**

交换机首次加电启动时，在它的运行配置文件中有缺省的配置数据。交换机的缺省名称为 Switch，控制台或虚拟终端(Virtual Teletype Terminal，VTY)线路都没有设置密码。对于本实验所用交换机，可以用 show run 命令来显示交换机的缺省配置。

(2) 交换机端口属性：Switch# **show interface FastEthernet 0/1**

使用 show interface 命令可以看到接口的属性。缺省情况下，交换机的端口(接口)设置为自动模式(Auto Mode)，即它会自动探测半双工或全双工操作模式以及端口的速率，如 10Mb/s 或 100Mb/s。

(3) VLAN 属性：Switch# **show vlan**

缺省情况下，交换机的所有端口初始化时都属于 VLAN1，VLAN1 作为缺省管理 VLAN。使用 show vlan 命令可以显示交换机中所定义的 VLAN 的相关信息。

(4) 闪存目录：Switch# **directory flash**

由于新交换机还没有配置过，它的闪存目录(Flash Directory)里没有包含任何 VLAN 数据库文件(vlan. dat)，也没有保存的配置文件(config. text)。其中，vlan. dat 文件用来存储本地 VLAN 的信息，交换机使用该文件与其他交换机共享 VLAN 的信息。缺省情况下，闪存目录里有一个包含 IOS 映像的文件(以. bin 结尾)、一个称为 env_vars 的文件以及一个称为 html 的子目录。

（5）显示 IOS 版本信息：Switch＃**show version**

使用该命令可以验证 IOS 版本和配置寄存器的设置。另外，在该输出中还可以看到交换机的其他信息，如 IOS 系统映像文件名、交换机型号、序列号码、内存大小以及端口号码和类型。

4）交换机的网络配置

交换机的配置模式从特权 EXEC 模式进入。在命令行界面，缺省的特权 EXEC 模式提示符为 Switch＃。

（1）配置设备特权模式口令。

```
Switch>                          //进入用户模式
Switch>enable                    //从普通模式进行特权模式
Switch# configure terminal       //进入配置模式，可简写(conf t)
```

（2）指定交换机的主机名和密码。

安全性、文档和管理对于每一台互联网络设备都是非常重要的。每台交换机都应该配置一个主机名，都应该在控制台和虚拟终端线路上设置密码。下面的命令行可用来设置交换机的主机名和密码保护的线路。

```
Switch(config)#hostname c2950-A          //为交换机命名，在远程登录时这个很有用
c2950-A(config)#line configuration 0
c2950-A(config-line)#password
c2950-A(config-line)#login
c2950-A(config-line)#line vty 0 4
c2950-A(config-line)#password
c2950-A(config-line)#login
```

（3）指定交换机的 IP 地址和缺省网关。

为了使交换机能够被 Telnet 和其他 TCP/IP 应用所访问，需要给交换机设置 IP 地址和缺省网关。缺省情况下，VLAN1 是管理 VLAN（Management VLAN）。在基于交换的网络中，所有网络设备都应该属于同一个管理 VLAN。这样，仅用一台管理工作站就可以访问、配置和管理所有网络设备。

```
Catalyst 2950
c2950-A(config)#interface VLAN1                          //进入 vlan1，本征 vlan
c2950-A(config-if)#ip address 192.168.1.10 255.255.255.0  //配置交换机的管理 IP
c2950-A(config-if)#ip default-gateway 192.168.1.1         //配置默认网关
c2950-A (config-if)#noshutdown                            //激活本征 vlan1
```

（4）设置端口属性。

交换机快速以太网端口缺省设置为自动速度（Auto-Speed）和自动双工模式（Auto-Duplex），这样使得接口可以协商这些设置。当网络管理员需要保证某个接口使用特定的速率和双工模式（半双工或者全双工）时，这些值可以手动设置。

```
c2950-A(config)# interface FastEthernet0/2
c2950-A(config-if)# duplex full
c2950-A(config-if)# speed 100
```

# 实验 3　单个交换机 VLAN 的划分

**1. 实验目标**

(1) 掌握单交换机划分 VLAN 的基本设置。

(2) 根据网络模型示意图连线,实现单交换机的 VLAN 划分。

**2. 实验准备**

Cisco Catalyst 2950 交换机一台,PC 两台,直连网线两根。

**3. 实验内容**

1) 实验要求

如图 4-14 的网络模型示意图所示,有一台交换机 c2950-A,要求把 PC2 划分在一个 VLAN 中,VLAN 的号是 2,VLAN 的名字是 No2。并验证 PC1 和 PC2 之间的通信情况。

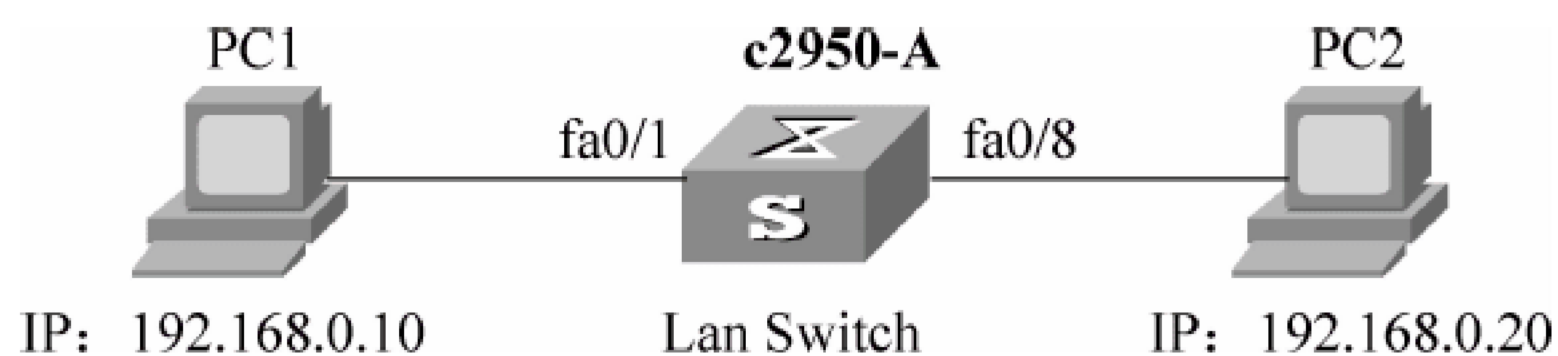



图 4-14　单交换机 VLAN 划分

2) 相关命令

在同一个交换机上进行 VLAN 划分时会使用到的相关配置命令如下。

(1) vlan database: 进入 VLAN 数据库。

(2) vlan <vlan 号> [name <vlan 名>]: 创建 VLAN。

(3) switchport mode access: 设置端口为存取模式。

(4) switchport access vlan <vlan 号>: 将端口添加到 VLAN。

(5) show vlan: 显示 VLAN 信息。

3) 创建单交换机的 VLAN

(1) 在交换机的特权模式下,输入 show vlan,查看当前 VLAN 状态:

```
c2950-A# show vlan
  VLAN Name                          Status    Ports
  ---------------------------------------------------------------------------
  1    default                       active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                               Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                               Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                               Fa0/13, Fa0/14, Fa0/15, Fa0/16
```

```
                                          Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                          Fa0/21, Fa0/22, Fa0/23, Fa0/24
 1002 fddi-default                 active
 1003 token-ring-default           active
 1004 fddinet-default              active
 1005 trnet-default                active
 ---------------------------------------------------------------------------------
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
 ---------------------------------------------------------------------------------
 1     enet   101001 1500  -   -   -   -     -   0     0
 1002  fddi   101002 1500  -   -   -   -     -   0     0
 1003  tr     101003 1500  -   -   -   -     -   0     0
 1004  fdnet  101004 1500  -   -   -   ieee  -   0     0
 1005  trnet  101005 1500  -   -   -   ibm   -   0     0
 c2950-A#
```

可以看出，默认设置下，所有的端口都在 VLAN1。

（2）在交换机的特权模式下，输入“vlan database”，进入 VLAN 数据库。

（3）在 VLAN 配置模式下输入“vlan 2”，创建一个标号为 2 的 VLAN。

```
c2950-A#vlan database
c2950-A(vlan)#vlan 2
VLAN 2 added:
    Name: No2
c2950-A(vlan)#
```

（4）输入“exit”，退到特权模式，再进入全局配置模式，输入“int fa0/8”，进入端口 8 的端口配置模式（c2950-A(config-if)#），输入“switchport mode access”，再输入“switchport access vlan 2”命令，将端口 8 加入到 VLAN2 中。

```
c2950-A(vlan)#exit
APPLY completed.
Exiting...
c2950-A#conf t
Enter configuration commands, one per line. End with CNTL/Z.
c2950-A(config)#int fa0/8
c2950-A(config-if)#switchport mode access
c2950-A(config-if)#switchport access vlan 2
c2950-A(config-if)#
```

（5）在 PC1 上利用 ping 命令验证与 PC2 之间的通信状态，证实不同 VLAN 内的计算机将无法通信。

（6）在端口 8 的端口配置模式（c2950-A(config-if)#）下，输入“no switchport access vlan 2”命令，可将端口 8 从 VLAN2 中删除。

（7）在 VLAN 数据库中的 VLAN 配置模式（c2950-A（vlan）#）下，输入“no vlan 2”，即可删除 VLAN2。

# 实验 4　跨交换机 VLAN 的划分

**1. 实验目标**

（1）掌握跨交换机划分 VLAN 时的基本设置。

（2）根据网络模型示意图示连线，实现跨交换机的 VLAN 划分。

**2. 实验准备**

Cisco Catalyst 2950 交换机两台，PC 两台，直连网线两根，交叉网线一根。

**3. 实验内容**

1）实验要求

如图 4-15 的网络模型示意图所示，有两台交换机 c2950-A 和 c2950-B，要求把 PC3、PC4 划分在一个 VLAN 中，VLAN 的号是 3，VLAN 的名字是 No3。

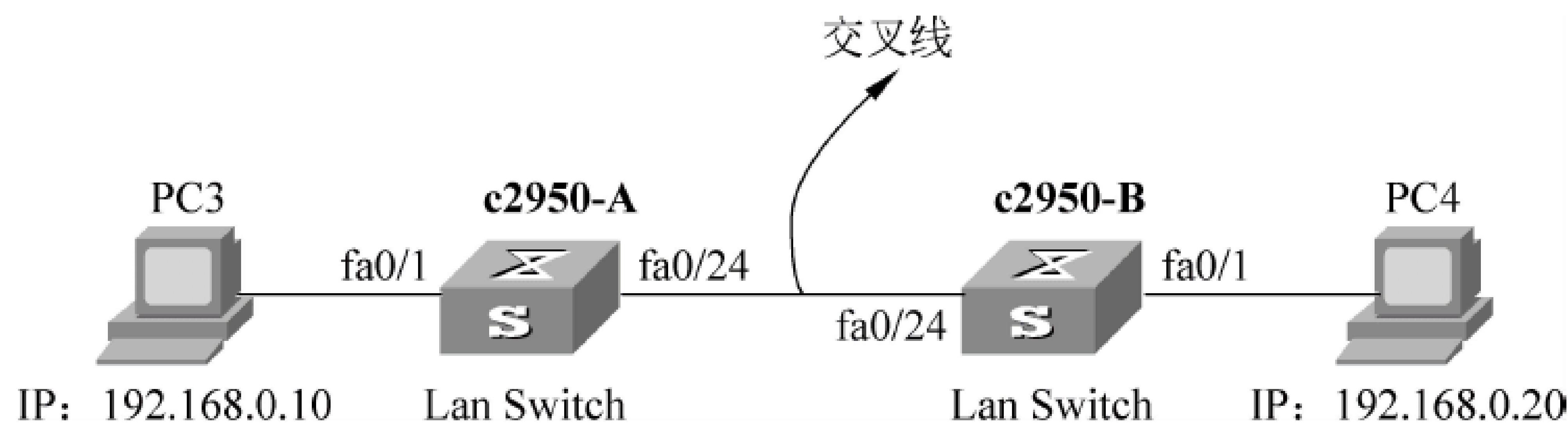



图 4-15　跨交换机 VLAN 划分

2）相关命令

在跨交换机上进行 VLAN 划分时会使用到的相关配置命令如下。

（1）vtp domain<域名>：设置 VTP 域名。

（2）switchport mode trunk：将交换机的级联口 trunk 打开。

（3）show vtp status：显示 VTP 状态。

（4）show spanning-tree vlan <vlan 号>：显示 VLAN 的 spanning-tree 信息。

3）创建多交换机间的 VLAN

（1）在交换机 c2950-A 的特权模式下，输入“vlan database”，进入 VLAN 数据库。

（2）在 VLAN 配置模式下，输入“vtp domain vd1”，设置一个 VTP 的域名 vd1。

（3）输入“vlan 3”，创建一个标号为 3 的 VLAN：

```
c2950-A# vlan database
c2950-A(vlan)# vtp domain vd1
Changing VTP domain name from NULL to vd1
c2950-A(vlan)# vlan 3
```

```
  VLAN 3 added:
    Name: No3
c2950-A(vlan)#
```

（4）输入“exit”，退到特权模式，再进入全局配置模式，输入“int fa0/1”，进入端口 1 的端口配置模式（c2950-A(config-if)#），输入“switchport mode access”，再输入“switchport access vlan 3”命令，将端口 1 加入到 VLAN3 中：

```
c2950-A(vlan)#exit
APPLY completed.
Exiting...
c2950-A#conf t
Enter configuration commands, one per line. End with CNTL/Z.
c2950-A(config)#int fa0/1
c2950-A(config-if)#switchport mode access
c2950-A(config-if)#switchport access vlan 3
c2950-A(config-if)#
```

（5）输入“int fa0/24”，进入端口 24 的端口配置模式（c2950-A(config-if)#），输入“switchport mode trunk”，打开 trunk 功能：

```
c2950-A(config)#int fa0/24
c2950-A(config-if)#switchport mode trunk
c2950-A(config-if)#
```

（6）在另一台交换机 c2950-B 上重复以上步骤，将其端口 1 也加入到同一个 VLAN（VLAN3）中，并将端口 24 的 trunk 功能打开。

（7）在 PC3 上利用 ping 命令验证与 PC4 之间的通信状态，证实不在同一台交换机上的相同 VLAN(VLAN3)内的计算机可以相互通信。

（8）将 PC3 的网线从 fa0/1 中拔出来插入交换机 c2950-A 的另一个端口（即 VLAN1）中，在 PC3 上再次利用 ping 命令验证与 PC4 之间的通信状态，证实不同 VLAN（VLAN1 和 VLAN3）内的计算机间无法通信。

（9）在特权模式（c2950-A#）下输入“show vlan”，显示 VLAN 信息；输入“show vtp status”，显示 VTP 状态。

（10）在特权模式（c2950-A#）下输入“show spanning-tree vlan 3”，显示 VLAN 的生成树信息。

## 思考与练习

### 一、填空题

1. 将传输介质的频带有效地分配给网上各节点的方法称为________方法。

2. IEEE 802.3 以太网帧是变长的，有效的 MAC 帧的大小在________字节到________字节之间。

3. 局域网的数据链路层又划分为________子层和________子层。

4. 区别以太网设备的标识为 MAC 地址，它的总长度为________比特。

5. 在 Windows 中，通常可以使用________命令查看 MAC 地址。

6. 在计算机网络和数据通信中最常用的检错码是________码。

7. CRC 码有两个重要特性，分别是________性和________性。

8. 从技术角度讲，实现 VLAN 的划分通常有三种方法：基于________的 VLAN 划分、基于________的 VLAN 划分和基于________的 VLAN 划分。

**二、选择题**

1. 决定局域网性能的主要因素不包括(　　)。

A. 网络拓扑结构　　B. 网络传输介质

C. 介质访问控制方式　　D. 网络通信模型

2. 在以太网中广泛应用的是(　　)位的 CRC 码。

A. 16　　B. 32　　C. 64　　D. 128

3. IEEE 802 标准提供的介质访问控制方式不包括(　　)。

A. Token Bus　　B. Token Ring　　C. ALOHA　　D. CSMA/CD

4. 下面关于以太网、令牌环网和令牌总线网的比较，说法不正确的是(　　)。

A. 以太网适用于各种负载的应用

B. 令牌总线网是在物理总线上建立一个逻辑环

C. 令牌总线网和令牌环网没有冲突

D. 重负载时令牌环网的效率最高

5. VLAN 的功能不包括(　　)。

A. 抑制广播风暴　　B. 简化项目管理或应用管理

C. 增加网络连接的灵活性　　D. 限制冲突域

**三、思考题**

1. 什么是局域网？局域网的工作特点是什么？

2. 局域网的介质访问控制方式有哪几类？分别有何优缺点？

3. 介绍 IEEE 802.3 帧的结构及其中每一个字段的功能。

4. 为什么 IEEE 802.3 以太网中，有效的 MAC 帧的大小要控制在 64～1518 字节之间？

5. 已知要发送的信息位为 100101110010，收发双方约定的使用生成多项式 $G(x)=X^4+X^2+1$，求循环冗余校验码。

6. 什么是 VLAN？VLAN 有哪些优点？

7. VLAN 有几种实现方法？分别有何特点？

8. 什么是无线局域网？简要介绍无线局域网 IEEE 802.11 系列标准。

第 5 章

# 网络层的主流协议

TCP/IP 的网络层被称为网络互连层或网际层(Internet Layer),是以数据报形式向传输层提供面向无连接的服务。网络层的主要协议包括 IP 协议、ARP 协议、RARP 协议、ICMP 协议等。

## 5.1 IP 协 议

IP 协议是 Internet Protocol 的缩写,是 TCP/IP 体系中最重要的协议,其定义了用以实现面向无连接服务的网络层分组格式,其中包括 IP 寻址方式。不同网络技术的主要区别在数据链路层和物理层。而 IP 协议则能够将不同的网络技术在 TCP/IP 的网络层进行统一,以统一的 IP 分组传输提供对异构网络互连的支持。IP 协议使互连起来的许多计算机网络能够通信,在 Internet 中实现网络互连正是采用了 TCP/IP 协议族中的 IP 协议。IP 协议是为计算机网络相互连接进行通信而设计的协议,并通过采用 IP 协议可以屏蔽低层网络的差异,所有的网络都使用 TCP/IP 协议,使用同一种网络语言。IP 地址可以实现不同网络的互连以及不同网络中不同主机之间的互连。

因此,TCP/IP 体系中的网络层常常被称为网际层(Internet Layer)或 IP 层。由于 IP 协议实现的是面向无连接的数据报服务,故 IP 分组通常又被称为 IP 数据报,一个 IP 数据报由首部和数据两部分组成。

在传送数据报时,高层协议将数据传给 IP 协议,IP 协议将数据封装为 IP 数据报后通过网络接口发送出去。如果目的主机直接连在本地网中,则 IP 协议直接将数据报传送给本网的目的主机;如果目的主机是在远程网络上,则 IP 协议将数据报传送给本地路由器,由本地路由器将数据报传送给下一个路由器或目的主机。这样,一个 IP 数据报通过一组互联网络从一个 IP 实体传送到另一个 IP 实体,直至达到目的地。

IP 数据报由报头和报文数据两部分组成,如图 5-1 所示。

IP 数据报中各个字段的含义简要说明如下。

(1) 版本:4 位,IP 协议的版本号,IPv4 版本取值为 4。

(2) IP 报头长度(Internet Header Length,IHL):4 位,以 32 位为单位表示的报头

长度。

(3) 服务级别(Terms of Service,ToS):8 位,用于规定优先级、传送延迟、吞吐量和可靠性等参数。

(4) 报文长度:16 位,以字节为单位表示的报文总长度(包括报头和数据两部分)。

(5) 标识(IDentity,ID):16 位,数据报的唯一标识,用于数据报的分段与重装。

(6) 标志:3 位,数据报是否分段的标志。

(7) 分段偏移:13 位,以 64 位为单位表示的分段偏移。

(8) 生存期(Time To Live,TTL):8 位,允许数据报在网间传输的存活时间。

(9) 上层协议号:8 位,指出发送数据报的上层协议。

(10) 报头校验和:16 位,仅用于对报头的正确性检查。

(11) 源 IP 地址:32 位,发送数据报的源主机 IP 地址。

(12) 目的 IP 地址:32 位,接收数据报的目的主机 IP 地址。

(13) 任选项:可变长度,提供任选的服务,如时间戳、错误报告及特殊路由等。

(14) 填充:可变长度,保证 IP 报头以 32 位为边界对齐。

Internet 中的互连设备多是路由器。路由器可以把互连以后的网络看做一个虚拟网络,即一个采用 IP 协议、IP 逻辑地址的逻辑网络。从 Internet 用户的角度来看,这个网络就像是一个统一的网络,看不到逻辑网络里面存在的差异,也不必关心网络内部的构成等问题。

<table>
<tr><td>0</td><td>4</td><td>8</td><td colspan="2">16　　　24</td><td>31</td></tr>
<tr><td>版本</td><td>IHL</td><td>服务级别</td><td colspan="3">报文长度</td></tr>
<tr><td colspan="3">标识</td><td>标志</td><td colspan="2">分段偏移</td></tr>
<tr><td colspan="2">生存期</td><td>上层协议号</td><td colspan="3">报头校验和</td></tr>
<tr><td colspan="6">源IP地址</td></tr>
<tr><td colspan="6">目的IP地址</td></tr>
<tr><td colspan="6">任选项+填充</td></tr>
<tr><td colspan="6">数据</td></tr>
</table>

图 5-1　IP 数据报格式

## 5.1.1　IP 地址

众所周知,地球有几十亿人口,如何能在茫茫人海当中精确地找到一个人?采用的方法是找到这个人的住址就能确定找到这个人,因为每个人的住址都是唯一的。同样的,在 Internet 中的主机也数以亿计,那么如何能够寻找到特定的主机呢?答案就是要通过 IP 地址找到特定主机。也就是说 IP 地址要在本网络当中能唯一地表示一台主机。因此,IP 地址具有唯一性。

就像生活在地球上的每个人都有一个唯一的住址与其对应，那么在 Internet 上的每台主机都有一个唯一的 IP 地址与其对应。IP 协议就是使用这个地址在主机之间传递信息，这也是 Internet 能够运行的基础。

IP 地址是分配给主机的逻辑地址，这种逻辑地址在互联网中表示唯一主机，它独立于任何特定的网络硬件和网络配置。逻辑地址在整个互联网中有效，不管物理网络的类型如何，IP 地址都有相同的结构。那么，IP 地址有什么作用？IP 是如何表示的，又有什么样的层次结构呢？

**1. IP 地址的作用**

以太网利用 MAC 地址（物理地址）标志网络中的一个节点，两个以太网节点的通信最主要是需要知道对方的 MAC 地址。但是，以太网并不是唯一的网络，世界上存在着各种各样的网络，这些网络使用的技术不同，物理地址的长度、格式和表示方法也不相同。因此，如何统一节点的地址表示方式、保证信息跨网传输是互联网面临的一大难题。

显然，统一物理地址的表示方法是不现实的，因为物理地址表示方法是和每一种物理网络的具体特性联系在一起的。因此，互联网对各种物理网络地址的“统一”必须通过上层软件完成。确切地说，互联网对各种物理网络地址的“统一”就要在 IP 层（网络层）完成。

**2. IP 地址的表示**

IP 协议提供了一种互联网通用的地址格式，IP 地址由 IP 地址管理机构进行统一管理和分配，保证互联网上运行的设备（如主机、路由器等）不会产生地址冲突。IP 地址由 32 个二进制位表示，但是二进制格式对于普通用户来说使用比较麻烦。因此，对于普通用户来讲，仍然是十进制数更容易接受。因此，IP 地址采用了通用的“点分十进制”的方法来表示。具体如下：将 32 个二进制数分成 4 组（每组 8 位，即 1 个字节），并将每组转换成十进制数（由二进制与十进制的转换知识，可以断定范围是在十进制数 0～255 范围内），且每组间用圆点来分隔。因此，IP 地址可以简单表示为 *W*.*X*.*Y*.*Z* 的形式，如图 5-2 所示。

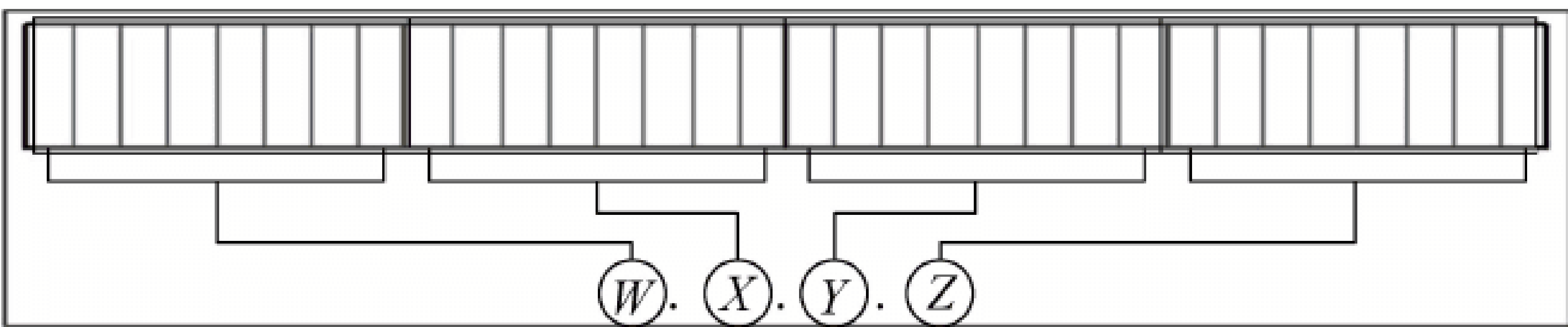



图 5-2　IP 地址的表示方法

具体举例如图 5-3 所示。

| 二进制格式 | 10000011 01101011 00000011 00011000 |
|---|---|
| 十进制格式 | 131 . 107 . 3 . 24 |

图 5-3　IP 地址举例

### 3. IP 地址的层次结构

一个互联网包括了多个网络,而一个网络又包括了多台主机,因此,互联网是具有层次结构的,与互联网的层次结构相对应,互联网使用的 IP 地址也采用了层次结构。这种层次结构就是指 IP 地址由网络号(net-id)和主机号(host-id)两个层次组成。这种层次结构对于初学计算机网络的人来说,可能比较复杂难懂,举出如下例子:IP 地址的这种层次结构可以与我们日常生活中的电话号码非常类似。电话号码通常由电话区号与电话号码,类比之后可以如图 5-4 所示。




图 5-4 IP 地址与电话号码类比图

网络号可以类比电话区号,电话区号是用来表示这台电话机所在的地区,主机号可以类比电话号码。例如图 5-4 中的"0411"指的是这台电话机在辽宁省大连地区,而图中"86729742"指的就是这台电话机占用了大连地区的一个唯一号码。而 IP 地址中的网络号可以表示这台 IP 地址标识的主机所在的是哪一个网络,而 IP 地址中的主机号就是用来表示这个 IP 地址所对应的主机在这个网络中的位置,因此,IP 地址的这种层次结构明显地携带了位置信息。如果给出一个具体的 IP 地址,马上就能知道这个 IP 地址所对应的主机位于哪个网络,这给互联网的路由选择带来了很大好处。由于 IP 地址不仅包含了主机本身的地址信息,而且还包含了主机所在网络的地址信息,因此,在将主机从一个网络移动到另一个网络时,主机 IP 地址必须进行修改以正确地反映这个变化。例如,一台主机具有 IP 地址 192.168.1.3,这台主机如果需要移动到另一个网络的话,就必须分配另一个 IP 地址,否则就不可能与互联网上的其他主机正常通信。这种方式与生活中的住址非常相似,住址标识了一个人的位置信息,而这种住址信息也与 IP 地址一样具有一些层次结构(城市、区、街道号码等),如果一个人从一个地区搬到另一个地区,那么住址就要发生改变,否则就无法正常与别人通信往来。

### 4. IP 地址的使用规则

1) 主机 ID 的使用规则

主机 ID 使用规则可以简单归纳为一个唯一,三个禁用,具体如下。

(1) 同一网络中,主机 ID 是唯一的。如果主机 ID 不唯一,就引发 IP 地址冲突,地址冲突的两台主机不能利用网络进行通信。

(2) 主机 ID 各位不能全为"1"。因为这标识了广播地址。例如 202.112.144.255 标识了该网络上的所有主机;当该网络的某台主机需要发送信息给所有该网络的主机时,就使用此地址。

(3) 各位不能全为"0"。这标识了一个网络。例如 IP 地址 202.112.144.0,意味着标识"202.112.144"这个 C 类网络。

(4) "127.0.0.1"不能分配给网络上的任何计算机使用,因为它代表本地主机的 IP 地址。

2）IP 地址的使用规则

（1）在 Internet 中 IP 地址的分配应该由指定的机构进行；但在局域网中 IP 地址的分配可以不受限制。若在局域网中配置 IP 地址，需要遵循以下原则。

（2）同一个网络内的所有主机必须分配相同的网络地址；同一个网络内的所有主机必须分配不同的主机地址。若计算机 A 和计算机 B 都接入了同一个网络，计算机 A 若分得了 IP 地址 202.116.94.4，那么计算机 A 和计算机 B 都应该享有 202.116.94.0 这个网络号，且计算机 B 在被分配 IP 地址时，应该在 202.116.94.1～202.116.94.254 中除了 202.116.94.4 之外都可以选择。

（3）不同网络内的主机必须分配不同的网络地址，但是可以分配相同的主机地址。若计算机 A 分配了 IP 地址 202.116.94.5，那么如果计算机 B 与计算机 A 不在一个网络中，那么计算机 B 可以使用 202.116.95.5。也就是说计算机 A 处于 202.116.94.0 的网络，并分配了主机号“5”，那么计算机 B 是在 202.116.95.0 的网络，并也分配了主机号“5”。也就是说计算机 A 与计算机 B 处于不同的网络，但是主机号可以相同，这并不影响 IP 地址的唯一性原则。

（4）IP 地址必须结合子网掩码一起使用。

综上所述，不能使用的 IP 地址可以归纳为 0.0.0.0、255.255.255.255、127.x.x.x、A.0.0.0、A.255.255.255、B.B.0.0、B.B.255.255、C.C.C.0、C.C.C.255。

**5. IP 地址的分类**

前面已经讲过，IP 地址一共由 32 位二进制数表示，IP 地址由网络号与主机号组成。那么这 32 位二进制数哪些用来标识网络号，哪些用来标识主机号呢？这个问题比较复杂，但是弄清楚这个问题可以解决很多问题。因为只有当这些问题解决之后，才能够弄清楚下面两个问题。

（1）若网络号为 $m$ 位，则一共可以表示出 $2^m$ 个网络。

（2）若主机号为 $n$ 位，则能表示每个网络中可以容纳 $2^n-2$ 台主机。

由上面的分析可以得出，根据网络号位数的不同，主机的位数也不同，那么网络的规模也不同。即网络号位数越大，主机号位数越小。主机号位数越大，那么网络中容纳的主机个数越多，网络的规模也就越大；主机号位数越小，则网络规模越小，因此不同种类的网络规模也相差很大。也就是说有的网络可以容纳上万台主机，有的网络可能只能容纳几台主机。因此，为了适应各种网络规模的不同，将 IP 地址分为 A、B、C、D 和 E 这 5 类，它们分别使用 IP 地址的前几位加以区分，如图 5-5 所示。从图中可以看出，利用 IP 地址的前 4 位不同可以分辨出 IP 地址类型。但事实上，只需利用前两位就能判断出来，因为 D 类和 E 类地址很少使用。

每类地址所包含的网络数与主机个数不同。A 类 IP 地址用 7 位二进制数位来表示网络号位，其余 24 位标识主机号位，因此，由上面的分析得出，A 类 IP 地址标识的网络能够容纳 $2^{24}-2$ 台主机，所以，A 类的网络的规模最大，可以适用于大型网络。B 类 IP 地址用 16

位来表示主机号位，这样的网络共能容纳 $2^{16}-2$ 台主机，因此 B 类 IP 地址用于中型网络。C 类 IP 地址用 8 位表示主机号位，因此这样的网络共能容纳 $2^{8}-2$ 台主机，主要用于小型网络。D 类地址用来广播发送数据包，E 类地址则保留为以后所使用。IP 地址的分类情况如图 5-5 所示。

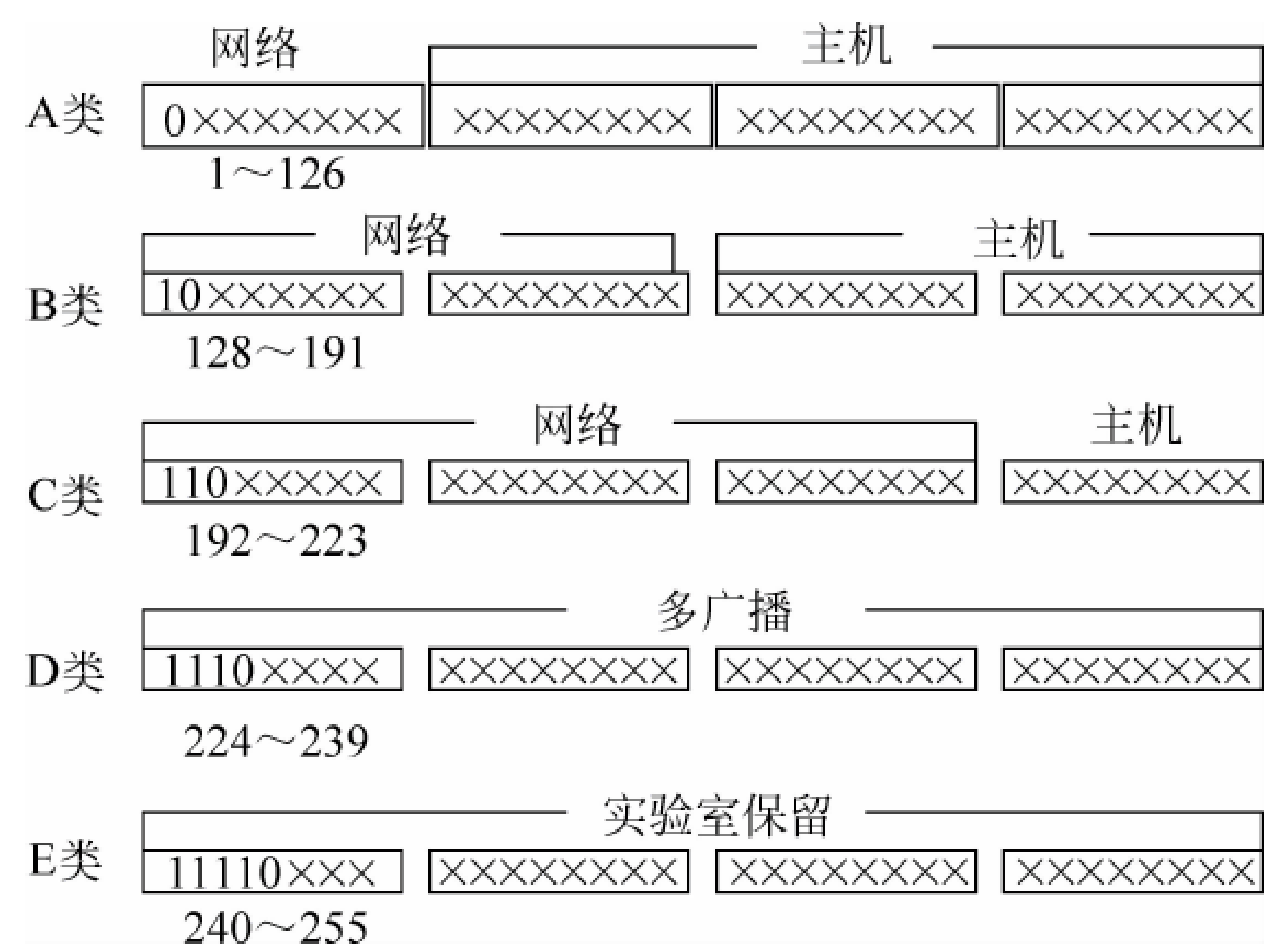



图 5-5 IP 地址的分类

IP 地址的内容非常复杂，IP 地址的分类不同，能够适应的网络规模也不同，因此 IP 地址的灵活性非常强。表 5-1 总结了 A、B、C 三类地址可以容纳的网络数和主机个数。

**表 5-1 各类 IP 地址对比表**

| 网络类别 | 用途 | IP 地址 | 网络 ID | 主机 ID | 网络取值范围 | 有效主机个数 |
|---|---|---|---|---|---|---|
| A | 大型网络 | *W*.*X*.*Y*.*Z* | *W* | *X*.*Y*.*Z* | 1～126 | 16 777 214 |
| B | 中型网络 | | *W*.*X* | *Y*.*Z* | 128～191 | 65 534 |
| C | 小型网络 | | *W*.*X*.*Z* | *Z* | 192～223 | 254 |

**6. 特殊的 IP 地址**

IP 地址除了可以表示主机的位置之外，还有几种特殊的 IP 地址，可以表示特殊的意义。

1) 网络地址

在很多时候，经常使用网络地址，那么如何用 IP 地址来表示网络呢？IP 地址中规定，IP 地址的“10”组合中可以包括一个非 0 的网络号与全 0 的主机号的组合，例如 57.0.0.0 这个 IP 地址，由前面的表述可以推断出这是一个 A 类 IP 地址，而 A 类 IP 地址后 24 位来标识主机号，而 57.0.0.0 这个 IP 地址中后 24 位主机号全为 0，这样的 IP 地址就可以标识一个网络。同样的 B 类 IP 地址后 16 位全为 0，也可标识为网络地址(例如 136.64.0.0)，C 类 IP 地址后 8 位全为 0，同样可以标识为网络地址(193.59.44.0)。而一个具有 IP 地址

192.163.8.56 的主机则可表示为这台主机处在 192.163.8.0 的网络，而它的主机号为 56。表 5-2 总结了 A、B、C 三类 IP 地址的网络规模详述。

**表 5-2　A、B、C 三类 IP 地址的网络规模详述**

| 网络类别 | 网络 ID 的取值范围 | 网络 ID 的始址和终值 | 网络个数 | 主机个数 |
|---|---|---|---|---|
| A | 1.*X*.*Y*.*Z*～126.*X*.*Y*.*Z* | 1.*X*.*Y*.*Z*～126.*X*.*Y*.*Z* | 126 | 约 1700 万 |
| B | 128.*X*.*Y*.*Z*～191.*X*.*Y*.*Z* | 128.0.*Y*.*Z*～191.255.*Y*.*Z* | 168 384 | 65 000 |
| C | 192.*X*.*Y*.*Z*～223.*X*.*Y*.*Z* | 192.*X*.*Y*.*Z*～223.*X*.*Y*.*Z* | 约 200 万 (2 097 152) | 254 |

2）广播地址

当一台设备想要向网络当中的所有主机发送数据包的时候，就产生了广播。为了使网络上所有设备能够注意到这个广播，必须使用一个可进行识别和侦听的 IP 地址。而这样的广播地址通常以主机号位全“1”结尾。广播有两种形式，一种为直接广播，另一种为有限广播。

(1) 直接广播

如果这个广播地址包含一个有效的网络号和一个全为“1”的主机号，那么就称其为直接广播地址。在 IP 互联网中，任意一台主机都可以向其他网络进行直接广播。

(2) 有限广播

如果 IP 地址当中的 32 位全为“1”即 255.255.255.255，那么这样的 IP 地址就称为有限广播地址，既然把它称为有限广播地址，就指的是它所产生的广播将限制在最小的范围内。如果采用标准的 IP 地址，那么有限广播将限制在本网络地址中；如果网络中划分了子网，那么有限广播将被限制在本子网中(见 5.1.2 节)。有限广播不需要知道网络号。因此，在不知道本机所处的是哪一个网络的时候，只能采用有限广播方式。

3）回送地址

网络地址 127.0.0.0 是一个保留地址，用于网络软件测试以及本地机器进程间通信。这个 IP 地址就被称为回送地址，无论什么程序，一旦使用了回送地址来发送数据，协议软件不进行任何网络传输，立即将之返回。因此，含有网络号 127 的数据报则不可能出现在任何网络上。

4）私有地址

Internet 保留了一部分地址用于用户创建自己的局域网或内部网时使用，不分配给任何主机，它们称为私有地址，也称内部 IP 地址。通常，A 类网络的私有地址范围为 10.0.0.1～10.255.255.254，B 类网络的私有地址范围为 172.16.0.1～172.31.255.254，C 类网络的私有地址范围为 192.168.0.1～192.168.255.254。

## 5.1.2　子网规划

### 1. 子网划分的原因

目前，我们不得不面对的问题是 IP 地址资源严重匮乏，而在实际的组网过程中，由于每

个网络中所含的主机数量不同,因此在分配 IP 地址的时候就很容易造成 IP 地址的浪费。例如,有 3 个不同的网络,每个网络的主机数分别为 A 网络容纳 40 台主机,B 网络容纳 120 台主机,C 网络容纳 240 台主机。其网络地址分别为 192.168.1.0,192.168.2.0 和 192.168.3.0,即使对于网络 A 也要至少给它分配一个 C 类地址,但其实一个 C 类网络可以容纳 254 台主机,因此严重浪费了 IP 地址。为了解决这种问题,可以将一个网络划分为一个个小的网络,而这些小网络就可以被称做为子网。

**2. 子网划分的方法**

前面已经讲到,IP 地址是由网络号和主机号组成。而通过划分子网,IP 地址将由网络号、子网号和主机号组成。经过网络号和主机号的再一次的层次划分,这些网络就能适应不同的网络规模。

为了避免 IP 地址的浪费,子网划分之后将主机号的部分进一步划分为子网号和主机号。经过子网划分之后,IP 地址就分为网络号、子网号和主机号三部分,如图 5-6 所示。

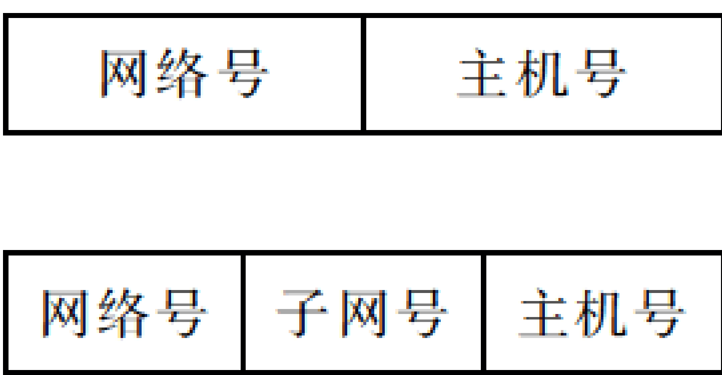



图 5-6 子网划分的层次结构

从图 5-6 中可以看出,为了创建一个子网,事实上网络管理员是从标准的 IP 地址中的主机号的位数中借出一些二进制位来标识子网的序号,这些二进制位就被称为子网号位。但是借位有以下两个原则。

(1) 要给主机号位至少留下 2 位。从前面的特殊 IP 地址可以看出,主机号全为“0”,或者全为“1”的 IP 地址,具有特殊意义。因此标准的 IP 地址主机号不能全为“0”或者“1”。如果借位之后主机号只剩下 1 位二进制位的话,那么就是非“0”即“1”,因此这违背了 IP 地址的使用规则。

(2) 子网号位数也要借出至少 2 位。通常网络号位也不是全为 0。

对于 A 类网络,主机号位一共 24 位,也就是说 A 类网络若划分子网最多只能用 22 位来表示子网号,同样的,B 类网络最多只能用 14 位创建子网,C 类网络最多只能用 6 位创建子网。

主机号位数借出一些二进制位来创建子网之后,主机号的位数变少了,因此相应的网络规模也会缩小。例如一个 C 类网络,它的主机号位数是 8 位,因此,C 类网络应该可以容纳 254 台主机($2^8-2$)。但要为一个 C 类网络的主机号位借出 3 位创建子网的话,主机号位就变为 5 位,因此,每个子网就能够容纳 30 台主机($2^5-2$)。那么这个 C 类网络所容纳的主机就明显减少了。下面我们来看一个实例。

例如:一个网络号为 192.168.1.0 的 C 类网络,从主机号中借出 3 位来表示子网号,如果子网号用 xxx 来表示,主机号用 yyyyy 来表示,即网络可以标识出:

11000000 10101000 00000001 xxxyyyyy

由于子网号全 0 和全 1 不能使用,因此子网的个数应该是 $2^3-2=6$ 个子网,且这 6 个子网的 IP 地址的范围如下:

(1) 11000000 10101000 00000001 00100001

～11000000 10101000 00000001 00111110(192.168.1.33～192.168.1.62),

子网号为 11000000 10101000 00000001 00100000,即 192.168.1.32。

(2) 11000000 10101000 00000001 01000001

～11000000 10101000 00000001 01011110(192.168.1.65～192.168.1.94),

子网号为 11000000 10101000 00000001 01000000,即 192.168.1.64。

(3) 11000000 10101000 00000001 01100001

～11000000 10101000 00000001 01111110(192.168.1.97～192.168.1.126),

子网号为 11000000 10101000 00000001 01100000,即 192.168.1.96。

(4) 11000000 10101000 00000001 10000001

～11000000 10101000 00000001 10011110(192.168.1.129～192.168.1.158),

子网号为 11000000 10101000 00000001 10000000,即 192.168.1.128。

(5) 11000000 10101000 00000001 10100001

～11000000 10101000 00000001 10111110(192.168.1.161～192.168.1.190),

子网号为 11000000 10101000 00000001 10100000,即 192.168.1.160。

(6) 11000000 10101000 00000001 11000001

～11000000 10101000 00000001 11011110(192.168.1.193～192.168.1.222),

子网号为 11000000 10101000 00000001 11000000,即 192.168.1.192。

在上面的实例中使用了 $2^n-2=6$(上例中 $n$ 为子网号位数)这样一个等式来计算子网数,实际上在分配 IP 地址或划分子网的时候经常会使用这个公式来计算可用的子网数以及每个子网内可用的主机数,公式就是 $2^n-2$,这个公式中 $n$ 表示的是主机号位数或者子网号位数,2 表示的是减去全“0”和全“1”的两个不可用的地址。具体意义如下。

(1) 如果 $n$ 为主机号位,公式 $2^n-2$ 即可得出网内主机个数 $N$。

(2) 如果 $n$ 为子网号位,公式 $2^n-2$ 即可得出子网个数 $N$。

**【注意】** 由前面的 192.168.1.0 的网络划分子网的实例,可以得出 192.168.1.32 等 6 个子网地址是不可以分配给任意一台主机作为 IP 地址的,因为它们已经不再表示任意一台主机,而表示的是一个子网,因此一个网络划分子网与不划分子网是有区分的,划分子网之后可能导致有些原本可以使用的 IP 地址无法使用。

根据上面的分析,可以得出子网划分的一些步骤。

(1) 确定需要多少个子网,每个子网需要容纳多少台主机,就可以定义每个子网的子网掩码,网络地址(网络号+子网号)的范围和主机号的范围。

(2) 利用公式 $N=2^n-2$ 可以确定子网号位数或者主机号位数。

(3) 将网络地址中子网号位变换所有可能的二进制位组合方式,在每种组合方式中网络号位与子网号位置“1”,而将主机号位置“0”,即可得出每个子网地址。

(4) 将第(3)步中得到的每一个子网地址中的主机号位除掉全 0 和全 1 的组合,即可得

到每个子网的可用 IP 地址范围。

### 3. 子网掩码

子网掩码(Subnet Mask)又叫网络掩码,它是一种用来指明一个 IP 地址的哪些位标识的是主机所在的子网,以及哪些位标识的是主机的掩码。子网掩码不能单独存在,它必须结合 IP 地址一起使用。

子网掩码也是一个 32 位二进制表示,是与 IP 地址结合使用的一种技术。它的主要作用有两个。一是用于屏蔽 IP 地址的一部分以区别网络标识和主机标识,并说明该 IP 地址是在局域网上,还是在远程网上。二是用于将一个大的 IP 网络划分为若干小的子网络。那么这些网络是怎样区分出来的呢?也就是说 IP 地址的网络号和主机号各是多少位呢?如果不指定,就不知道哪些位是网络号、哪些是主机号,也就无法区分出网络。这时就需要靠子网掩码来实现,具体是用 IP 地址与子网掩码 32 位二进制按位做逻辑与运算,结果就是网络号,也就可以得出是什么样的网络。

事实上,子网掩码的内在含义也是指将对应 IP 地址网络号位(包括子网号位)的位数全部置"1",对应 IP 地址主机号位的部分全部置"0"。所以只要知道一个 IP 地址,就可以很快得出这个 IP 地址对应的子网掩码。因此,根据前面简述的 IP 地址的分类知识,这三类 IP 地址的网络号位和主机号位都不同,因此可以得出这三类 IP 地址在标准的情况下的子网掩码。A 类、B 类和 C 类 IP 地址对应的子网掩码可以如图 5-7 所示。

11111111.00000000.00000000.00000000

| A 类 | network | host | | | 255.0.0.0 |
|---|---|---|---|---|---|

11111111.11111111.00000000.00000000

| B 类 | network | | host | | 255.255.0.0 |
|---|---|---|---|---|---|

11111111.11111111.11111111.00000000

| C 类 | network | | | host | 255.255.255.0 |
|---|---|---|---|---|---|

图 5-7 A、B、C 三类 IP 地址对应的子网掩码

### 4. 子网划分的实例

在图 5-8 中,给定一个 C 类 IP 地址:192.168.2.0,要根据以下的需求划分子网:A 网络中共有 23 台主机,B 网络中有 21 台主机,C 网络中有 10 台主机,D 网络中有 28 台主机,如何通过划分子网的方式来满足需求?

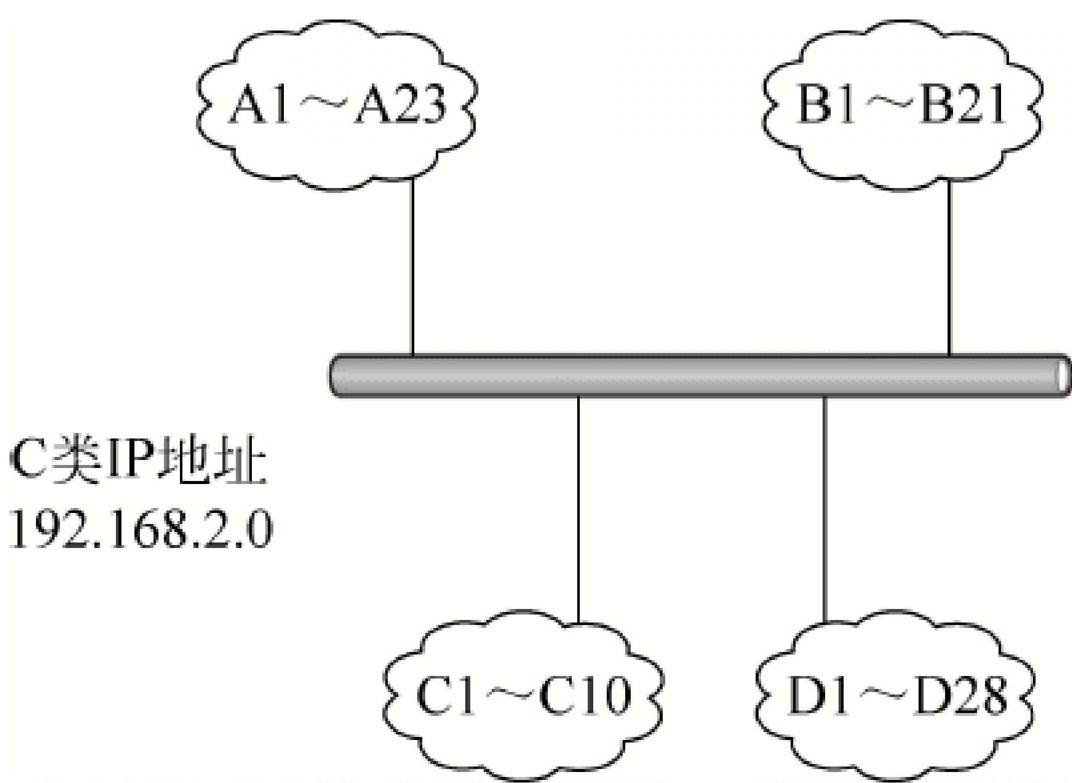



图 5-8 子网规划图

解析的步骤如下。

(1) 确定子网个数 4 个,主机的个数确定是以这 4 个子网中最大的主机个数为主,也就是主机个数确定为 28 台。

(2) 利用公式 $2^n-2$ 可以确定子网号位为 3 位，由于 C 类原本主机号位为 8 位，被子网号借去 3 位之后，主机号为 5 位。

(3) 将可能的所有的子网地址都列出来了，具体如下：

```
11000000 10101000 00000010 00100000 -- 192.168.2.32
11000000 10101000 00000010 01000000 -- 192.168.2.64
11000000 10101000 00000010 01100000 -- 192.168.2.96
11000000 10101000 00000010 10000000 -- 192.168.2.128
11000000 10101000 00000010 10100000 -- 192.168.2.160
11000000 10101000 00000010 11000000 -- 192.168.2.192
```

(4) 确定每个子网的可用 IP 地址范围，即去掉每个子网号内主机号位全 0 和全 1 的部分，具体如下：

```
192.168.2.33～192.168.2.62
192.168.2.65～192.168.2.94
192.168.2.97～192.168.2.126
192.168.2.129～192.168.2.158
192.168.2.161～192.168.2.190
192.168.2.193～192.168.2.222
```

这样，就将所有子网可用的 IP 地址表示出来，用户可以进行相应的设置。

**【注意】** 前面已经说过，每个 IP 地址都要匹配相应的子网掩码，本例中的子网掩码是将 IP 地址网络号位和子网号位置 1，主机号位置 0，而形成一个 32 位的二进制组合，即在本例中应该是这样的二进制组合：

11111111 11111111 11111111 11100000，点分十进制化简后得 255.255.255.224。

# 5.2　IPv6

随着 Internet 用户的迅速增加网络地址不足的危机日益严重，按目前入网主机的增长速度预计 IP 地址很快会被耗尽。Internet 面临的另一个问题是路由表规模的急剧膨胀。如不采取措施，在 IP 地址枯竭之前网络就会瘫痪。正是在这一背景下提出了新一代的 Internet 协议 IPv6 协议。

## 5.2.1　IPv4 的缺点

尽管目前使用的 IPv4 技术运用得非常普遍，但是仍然存在很多问题，随着 Internet 的迅猛发展，IPv4 的技术缺陷越来越明显，安全性等问题也越来越突出，主要表现在以下几个方面。

**1. 地址匮乏**

目前从理论上说，IP 地址一共可以有 $2^{32}=4\ 294\ 967\ 296$，即 42.9 亿个。这其中最大问题是网络地址资源有限，采用 A、B、C 三类编址方式后，可用的网络地址和主机地址的数目

大打折扣，以至目前的 IP 地址近乎枯竭。随着 Internet 上主机数目的迅速增加，地址空间难以满足未来移动设备以及消费类电子设备对 IP 地址的巨大需求。

**2. IP 地址分配不均衡**

目前 IP 地址没有合理的分配给各个国家和地区。其中，北美占有 3/4，约 30 亿个，其中美国占有绝大多数 IP 地址，并且大多数都是 A 类和 B 类 IP 地址。而人口最多的亚洲只有不到 4 亿个 IP 地址，我国只有 3 千多万个且大多是 C 类地址（适用于小型局域网），A 类和 B 类非常少。严重地制约了我国及其他国家互联网的应用和发展。

**3. 路由效率低下**

随着 ISP 数目的增长，已经出现路由表占满路由器内存，导致网络异常的恶性故障。如不采取措施，Internet 可能在地址枯竭之前就会瘫痪。同时 IPv4 地址的层次分配缺乏统一的分配和管理，它主要采用与网络拓扑结构无关的形式分配地址，这样就导致主干路由器中存在大量的路由表项，路由表越来越大就增加了路由器的工作量，降低了互联网服务的稳定性。庞大的路由表增加了路由查找和存储的开销，成为目前提高互联网效率的一个瓶颈。

**4. 安全性低**

互联网在最初的发展中并没有将安全方面的问题进行考虑，而随着互联网的普及与飞速发展，IPv4 并没有提供一些保证安全性的方法，难以满足目前互联网发展的需要。

**5. 移动性支持不够**

IPv4 在设计之初，对移动性考虑的不多，由于计算机移动技术的发展，移动网络的需求越来越多，而且安全性要求越来越高，而 IPv4 限制了移动技术发展。

## 5.2.2 IPv6 简介

如果说 IPv4 实现的只是人机对话，IPv6 则扩展到任意事物之间的对话，它不仅可以为人类服务，还将服务于众多硬件设备，如家用电器、传感器、远程照相机、汽车等，它将是无时不在、无处不在的深入社会每个角落的真正的宽带网。而且它所带来的经济效益将非常巨大。

**1. IPv6 特点**

（1）IPv6 具有更大的地址空间。IPv4 中规定 IP 地址长度为 32，即有 $2^{32}-1$ 个地址；而 IPv6 中 IP 地址的长度为 128，即有 $2^{128}-1$ 个地址。

（2）IPv6 使用更小的路由表。IPv6 的地址分配一开始就遵循聚类的原则，这使得路由器能在路由表中用一条记录表示一片子网，大大减小了路由器中路由表的长度，提高了路由器转发数据包的速度。

（3）IPv6 增加了增强的组播支持以及对流的支持，这使得网络上的多媒体应用有了长足发展的机会，为服务质量控制提供了良好的网络平台。

（4）IPv6 加入了对自动配置的支持。这是对 DHCP 协议的改进和扩展，使得网络（尤其是局域网）的管理更加方便和快捷。

(5) IPv6 具有更高的安全性。在使用 IPv6 网络中用户可以对网络层的数据进行加密并对 IP 报文进行校验，极大地增强了网络的安全性。

**2. IPv6 地址报文格式**

IPv6 报头格式如图 5-9 所示，报头各个字段含义如下。

(1) 版本号：4 位，表示 IP 协议的版本号，IPv6 版本取值为 6。

(2) 优先级：4 位，表示该数据报的优先级。

(3) 流标识：24 位，与优先级一起共同表示该数据报的服务质量级。

(4) 载荷长度：16 位，以字节为单位表示有效载荷长度。

(5) 下一个报头：8 位，表示第一个扩展报头的类型，或是上层 PDU 的含义。

(6) 跳步数：8 位，允许数据报跨越路由器的个数，表示该数据报在网间传输的最大存活时间。

(7) 源 IP 地址：128 位，发送数据报的源主机 IP 地址。

(8) 目的 IP 地址：128 位，接收数据报的目的主机 IP 地址。

| 0 | 4 | 8 | 16 | 24 | 31 |
|---|---|---|---|---|---|
| 版本号 | 优先级 | 流标识 | | | |
| 载荷长度 | | | 后续报头 | 步跳限制 | |
| 源IP地址(16字节) | | | | | |
| 目的IP地址(16字节) | | | | | |

图 5-9　IPv6 报头格式

**3. IPv6 地址格式**

在 IPv4 中，32 位的 IP 地址被分成网络号与主机号两部分。根据不同的地址类别，网络地址和主机地址所分配的位数是不同的。这种分配方式缺乏一定的灵活性。IPv6 的 128 位地址对此就没有做过多的类别限制，允许服务提供者根据实际需要进行地址划分。

IPv6 的 128 位的地址提供了很大的地址空间，但是使用二进制直接书写和记录必定十分不便。可以用类似于 IPv4 中使用点分十进制表示法来表示 IPv6 的 128 位地址。这种方法就是将 128 位的地址分成 8 个 16 位十六进制数，中间用冒号来分隔。其表示形式就是“A:A:A:A:A:A:A:A”，其中每个 A 代表一个 16 位二进制位，并使用十六进制表示，例如下面的 128 位的 IPv6 地址：3eef:1215:3216:4433:a213:b452:c019:ea87。

有些 IPv6 的地址包含了一长串的 0，为了进一步简化 IPv6 地址的表示，将每个十六进制数靠左边的多个连续的“0”省略不写，用双冒号来代表这些“0”，这成为一种双冒号表示法。

例如：6D3A:0:0:0:34AB:EE:56DC:3B2A 可以简化为 6D3A::34AB:EE:56DC:3B2A。

【注意】 为避免二义性，“::”在地址中只能出现一次。

**4. IPv6 地址类型**

IPv6 目前定义了三种地址单播地址、多播地址和任播地址，利用地址格式前缀来表示各种类型。

1）单播地址

单播地址指定了一个独立的主机。IPv6 定义了多种单播地址格式，如完整用户单播地址、NSAP(网络层服务访问点)地址、基于地理区域的地址、局部地址、与 IPv4 兼容的地址以及其他保留地址类型。完整单播地址格式如图 5-10 所示。

前 3 位是该地址类型的标识符

(1) REG ID 是 Internet 服务提供者的注册标识符。

(2) PROV ID 是提供者标识符。

(3) SUBSC ID 用于标识多个提供者所管理的用户。

(4) SUBNET ID 用于标识一个指定的子网。

(5) INTERFACE ID 用于标识一个单一接口。

| 010 | REG ID | PROV ID | SUBSC ID | SUBNET ID | INTERFACE ID |
|---|---|---|---|---|---|

图 5-10 IPv6 单播地址格式

如果 INTERFACE ID 是一个接口的全局唯一标识符，则可用它实现地址的自动生成。例如，一个节点通过监听路由器广播消息而发现了子网前缀，则可用 IEEE 802 MAC 地址作为 INTERFACE ID 来构造一个完整的 IPv6 地址。

局部地址用于定义子网中的局部网络，局部网络在未接入 Internet 之前可用局部地址进行访问操作。如果该局部网络要接入 Internet，可加入地址前缀(REG ID+PROV ID+SUBSC ID)，形成完整的 Internet 地址。

2）多播地址

多播地址标识了一组主机，以该地址类型传送的数据报将交付给地址对应的所有主机。IPv6 未定义广播地址类型，它可利用多播地址来实现。

3）任播地址

任播地址标识了一组接口，即该地址被分配给多个接口，当一个数据报发送给该地址时，只有按照路由协议计算出的最近的接口才接收该数据报。这种地址方式可用于标注一组服务提供者所对应的路由器，发送者利用路由扩展报头，将任播地址作为一个路由序列的一部分，从多个服务提供者中挑选一个来完成数据报传输。

**5. IPv4 到 IPv6 的过渡**

若要广泛地使用 IPv6，就必须将网络的基础设施升级以适应使用新协议的软件。IPv4 与 IPv6 的替换过程是漫长的，而不会像电话号码升级那么简单，有一个逐渐过渡的过程。目前运营商一般为 IPv4 网络，如果打算基于现有的 IPv4 网络来构建下一代互连网络，实现

从 IPv4 网络向 IPv6 网络的过渡，就需要考虑各种因素，不能对 IPv4 网络结构、性能和运行产生较大的影响和冲击，其主要原则如下。

(1) 保证现有投资的利益。目前网络上的主要设备包括：骨干路由器、汇聚路由器、接入路由器、以太网交换机和网络终端等，它们分别分布在不同网络层次中。应该根据网络具体情况，避免对已有用户或者网络有较大的冲击，包含用户现有投资。过渡方案的投资成本应该比较低。

(2) 保证两种网络之间业务的互通。目前 IPv4 网络已经有非常充足的用户群体，在向 IPv6 过渡过程中，将在局部出现大量的纯 IPv6 网络，为了避免“孤岛”效应，使这些独立的“IPv6 小岛”互通，就需要实现在现有的 IPv4 网络的基础上将“IPv6 孤岛”连接起来，并逐步扩大 IPv6 的实现范围。

(3) 保证现有 IPv4 业务的正常应用。从 IPv4 到 IPv6 的过渡必须是一个循序渐进的过程，在感受到 IPv6 带来的好处的同时，不应该对现有的 IPv4 业务造成影响。

(4) 保证过渡简单、易于操作。整个过渡过程无论是从网络过渡还是业务过渡，应该简单，易于操作。网络升级到 IPv6 后，路由器和主机应该仍然可以使用 IPv4 地址。

# 5.3　ARP 和 RARP

## 5.3.1　ARP 协议

### 1. ARP 协议的含义

IP 数据包常常通过以太网发送。以太网设备并不识别 32 位 IP 地址，它们是以 48 位以太网地址传输以太网数据包的。因此，IP 驱动器必须把 IP 目的地址转换成以太网目的地址。在这两种地址之间存在着某种静态的或算法的映射，常常需要查看一张表，这张表通常称为 ARP 表，而 IP 地址与物理地址(MAC 地址)的映射关系就称为 ARP 表项。地址解析协议(Address Resolution Protocol，ARP)就是用来确定这些映射的协议。

考虑一个网络上有两台主机 A 和 B，它们的 IP 地址分别是 IP1 和 IP2，物理地址分别为 MAC1 和 MAC2。在主机 A 需要将信息传送到主机 B 时，使用 IP1 和 IP2 做源地址和目的地址。但是信息的传递是按照网络体系结构自顶向下，因此必须利用下层的物理地址 MAC1 和 MAC2 来实现。那么，主机 A 如何将主机 B 的 IP 地址 IP2 映射到它的物理地址 MAC2 上呢?

将 IP 地址映射到物理地址的实现方法有很多种，地址解析协议 ARP 是以太网经常使用的映射方法，它主要是充分利用了以太网的广播能力，将 IP 地址与物理地址进行动态联编。

前面已经讲过，以太网最大的特点是具有强大的广播能力。针对这种具备广播能力、物理地址长并且长度固定的网络，IP 互联网采用动态联编的方法进行 IP 地址到物理地址的

映射。

简单地说，ARP 就是来解析对方物理地址的。结合前面的例子具体地说，当主机 A 向网络中广播一个 ARP 请求报文，报文中包含有目的主机 B 的 IP 地址，以请求主机 B 的物理地址。网络上所有的主机都能接收到这个 ARP 请求报文，接收到这个广播信息的主机把目标 IP 地址与自己的 IP 进行比较，其他主机发现目标 IP 不是自己的 IP 则不予回应，主机 B 发现目标 IP 与自己的 IP 地址相符，于是发送一个 ARP 响应报文，报告自己的物理地址。这样发送方主机 A 就得到了目的主机 B 的物理地址。

**2. ARP 的报文格式**

ARP 的报文格式如图 5-11 所示。

（1）物理网络类型字段是 2 个字节，表示源主机的物理网络类型。其中“1”代表以太网。

| 物理网络类型 |
|---|
| 协议类型 |
| 物理地址长度 |
| IP 地址长度 |
| 操作 |
| 源物理地址 |
| 源 IP 地址 |
| 目的物理地址 |
| 目的 IP 地址 |

图 5-11　ARP 报文格式

（2）协议类型字段是 2 个字节，表示发送方使用 ARP 获取物理地址的高层协议类型，其中“0x0800”代表 IP 协议。

（3）物理地址长度字段为 1 个字节，用于规定物理地址字段的长度。通常，物理地址字段占 6 个字节(48 位地址)。

（4）IP 地址长度字段为 1 个字节，用于规定 IP 地址字段的长度。通常，IP 地址字段占 4 个字节(IPv4 版本)。

（5）操作字段为 2 个字节，表示报文类型。其中 1 代表 ARP 请求报文，2 代表 ARP 响应报文，3 代表 RARP 请求报文，4 代表 RARP 响应报文。

（6）源物理地址字段为 6 个字节，用于存放发送方的物理地址。

（7）源 IP 地址字段为 4 个字节，用于存放发送方的 IP 地址。

（8）目的物理地址字段为 6 个字节，用于存放目的方的物理地址。对于 ARP 请求报文，该字段为空。

（9）目的 IP 地址字段为 4 个字节，用于存放目的方的 IP 地址。

**3. ARP 的工作原理**

下面我们将举例来讲解 ARP 协议的工作原理，如图 5-12 所示。

（1）主机 A 发送了一个带有目的主机 B 的 IP 地址请求信息包，请求主机 B 的 IP 地址 IP2 和物理地址 MAC2 的映射关系。

（2）以太网上所有的主机都会收到这个请求信息。

（3）只有主机 B 收到这个请求信息包之后，做出响应。向主机 A 发送带有自己 IP 地址 IP2 和物理地址 MAC2 的映射关系。

（4）主机 A 收到 IP2 与 MAC2 的映射关系，并可以在随后的发送过程中使用这个映射关系。

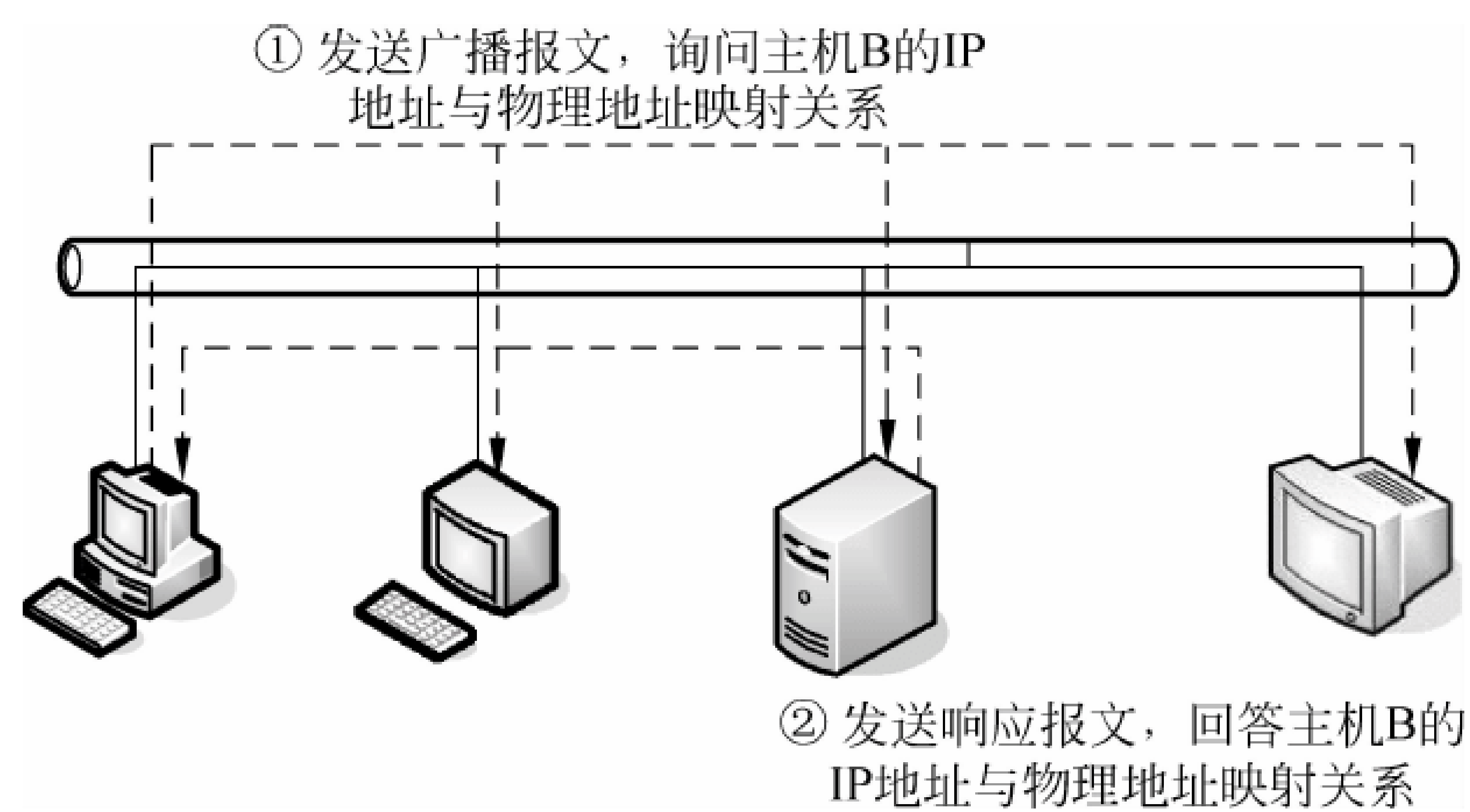



图 5-12　ARP 的工作原理

**4. ARP 协议的改进技术**

ARP 请求信息和响应信息的频繁发送和接收势必会对网络的工作效率产生影响。为了提高网络工作的效率，ARP 是可以采用一些改进技术。具体如下。

1）高速缓存技术

在每台使用 ARP 的主机中，都保留了一个专用的高速缓存区（Cache），用于保存已知的 ARP 表项。一旦收到了 ARP 应答，主机将获得的 IP 地址与物理地址的映射关系存入 Cache 的 ARP 表中。当发送信息时，主机首先到高速 Cache 的 ARP 表中查找相应的映射关系，若找不到再利用 ARP 进行地址解析。

这样，可以利用这种高速缓存技术，主机不必为每个发送的 IP 数据报使用 ARP 协议，这样就可以减少网络流量，提高处理的效率。若想查询自己主机中的 ARP 表项，非常简单。进入 DOS 模式下，输入 arp-a 命令，如图 5-13 所示。

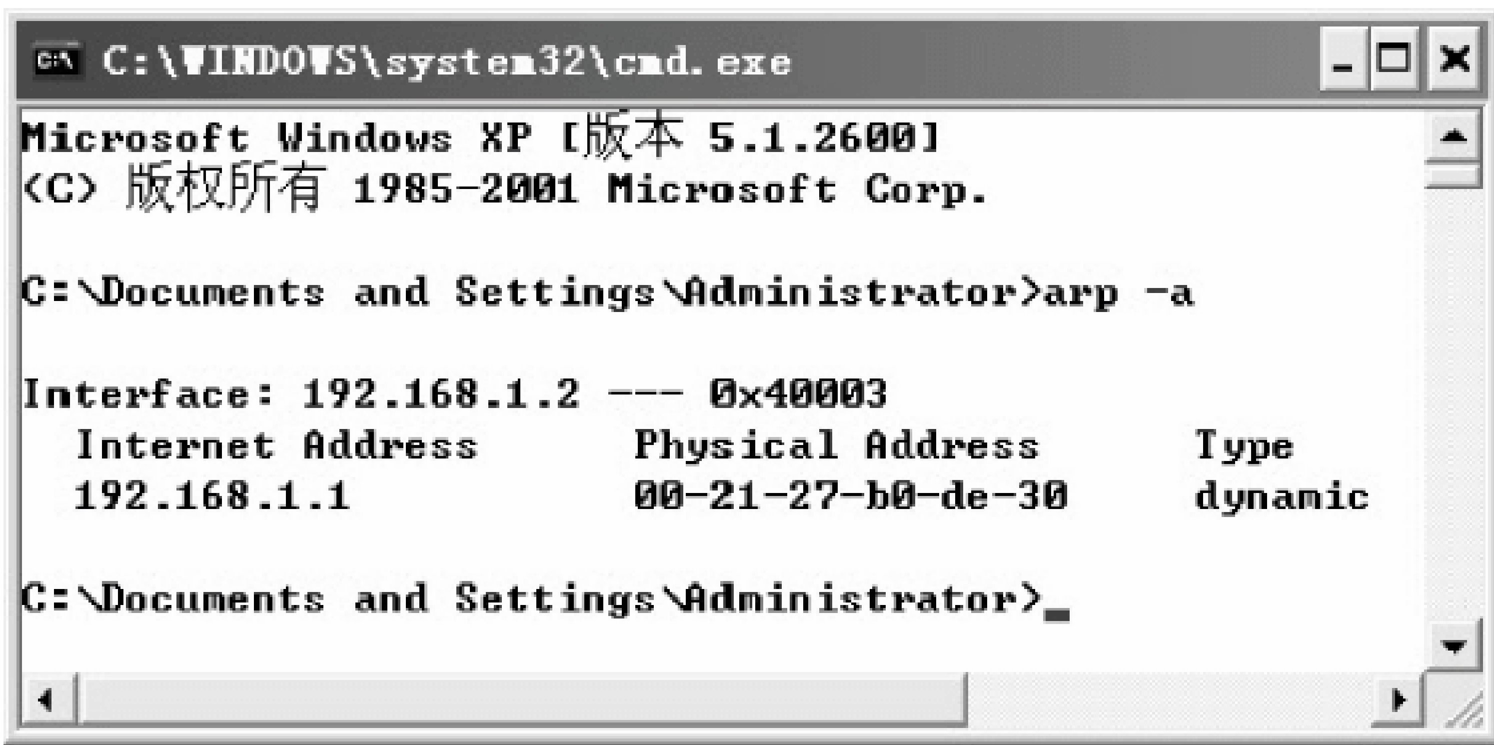



图 5-13　利用 arp-a 命令查询主机的 ARP 表项

2）其他改进技术

（1）在发送 ARP 请求时，数据报中包含了自己的 ARP 表项。目的主机就可以将这个 ARP 表项存储在自己的 ARP 表中，以备以后使用。这样可以防止目的主机为解析源主机的 ARP 表项而再发送一次 ARP 请求。

(2) 由于 ARP 请求时通过以太网广播出去的，因此，网络中所有主机都会收到这个 ARP 表项，那么这些主机都可以将源主机的 ARP 表项保存至各自的高速缓存区中，以备将来使用。

(3) 网络中的主机在启动时，可以主动广播自己的 ARP 表项，以尽量避免主机之间频繁进行 ARP 请求。

### 5.3.2 RARP 协议

**1. RARP 工作原理**

如果主机初始化之后只有自己的物理地址而没有 IP 地址，则可以通过 RARP 协议发送广播式请求报文来请求自己的 IP 地址，而 RARP 服务器负责对该请求做出应答。这样，没有 IP 地址的主机就可以通过 RARP 协议来获取自己的 IP 地址，RARP 的报文格式与 ARP 相同。当发送方以广播方式发送 RARP 请求报文时，在发送方物理地址字段和目的方物理地址字段上都填入本机物理地址。RARP 服务器主机接收到该请求报文后，便给发送方回送一个 RARP 响应报文，从目的方 IP 地址字段中带回发送方的 IP 地址。

**2. RARP 的工作过程**

RARP 的工作过程可以详细描述如下。

(1) 源主机发送一个本地的 RARP 广播，在此广播包中，声明自己的 MAC 地址并且请求任何收到此请求的 RARP 服务器分配一个 IP 地址。

(2) 本地网段上的 RARP 服务器收到此请求后，检查其 RARP 列表，查找该 MAC 地址对应的 IP 地址。

(3) 如果存在，RARP 服务器就给源主机发送一个响应数据包并将此 IP 地址提供给对方主机使用。

(4) 如果不存在，RARP 服务器对此不做任何的响应。

(5) 源主机收到从 RARP 服务器的响应信息，就利用得到的 IP 地址进行通讯；如果一直没有收到 RARP 服务器的响应信息，表示初始化失败。

## 5.4 ICMP 协议

Internet 控制报文协议(ICMP)，是一个工作在主机和路由器之间的消息控制和差错报告协议。路由器或其他设备一旦发现传输问题，就会分析其错误类型，并向源主机返回一个 ICMP 消息。IP 协议提供了无连接的数据报传送服务，在传送过程中，如果发生差错或意外情况，例如数据报目的地址不可达、数据报在网络中的滞留时间超过生存周期，中转节点或目的节点主机因为缓冲区不足而无法处理数据报等问题。就要通过一种通信机制，向源节点报告差错情况，以便源节点对差错进行相应的处理。这就是 ICMP 协议的意义所在。ICMP 与其他协议相比，具有一些比较鲜明的特点。

（1）ICMP 就像一个更高层的协议那样使用。然而，ICMP 是网络层的一个组成部分，并且所有 IP 模块都必须实现它。

（2）ICMP 用来报告错误，是一个差错报告机制。它为遇到差错的路由器提供了向最初源站报告差错的办法，源站必须把差错交给一个应用程序或采取其他措施来纠正问题。

（3）ICMP 不能用来报告 ICMP 消息的错误，这样就避免了无限循环。当 ICMP 查询消息时通过发送 ICMP 来响应。

（4）对于被分段的数据报，ICMP 消息只发送关于第一个分段中的错误。也就是说，ICMP 消息永远不会引用一个具有非 0 片偏移量字段的 IP 数据报。

（5）响应具有一个广播或组播目的地址的数据报时，永远不会发送 ICMP 消息。

（6）响应一个没有源主机 IP 地址的数据报时永远不会发送 ICMP 消息。也就是说，源地址不能为 0、一个回送地址、一个广播地址或者一个组播地址。

（7）ICMP 是两级封装的，每个 ICMP 报文放在 IP 数据报的数据部分中通过互联网传递，而 IP 数据报本身放在帧的数据部分中通过物理网络传递，具体如图 5-14 所示。




图 5-14　ICMP 的两级封装

### 5.4.1　ICMP 报文

ICMP 报文也分为报头区和数据区两部分，其中报头包含三个字段，如图 5-15 所示。

各字段含义如下。

（1）类型字段：用来标识报文，长度为 8 位。

（2）代码字段：提供有关报文类型的进一步消息，长度为 8 位。

（3）校验和字段：ICMP 使用与 IP 相同的相加校验算法，但 ICMP 校验和只覆盖 ICMP 报文，长度为 16 位。

| 类型 | 代码 | 校验和 |
| --- | --- | --- |
| ICMP 数据（取决于消息类型） | | |

图 5-15　ICMP 报文格式

ICMP 类型字段定义了报文的格式及意义，其类型如表 5-3 所示。

### 5.4.2　ICMP 差错报文

ICMP 差错报文包括目的地不可达到报文、超时报文、参数出错报文。

表 5-3　ICMP 报文类型

| 类 型 字 段 | ICMP 报文类型 | 类 型 字 段 | ICMP 报文类型 |
|---|---|---|---|
| 0 | 回送应答 | 12 | 数据报参数错误 |
| 3 | 目的地不可达 | 13 | 时间戳请求 |
| 4 | 源站抑制 | 14 | 时间戳应答 |
| 5 | 重定向 | 17 | 地址掩码请求 |
| 8 | 回送请求 | 18 | 地址掩码回答 |
| 11 | 数据报超时 | | |

**1. 目的地不可达到报文**

当一个路由器检测出一个数据报不能发往目的地时，路由器就会发送一个目的地不可达到报文。目的地不可达到报文格式如图 5-16 所示。

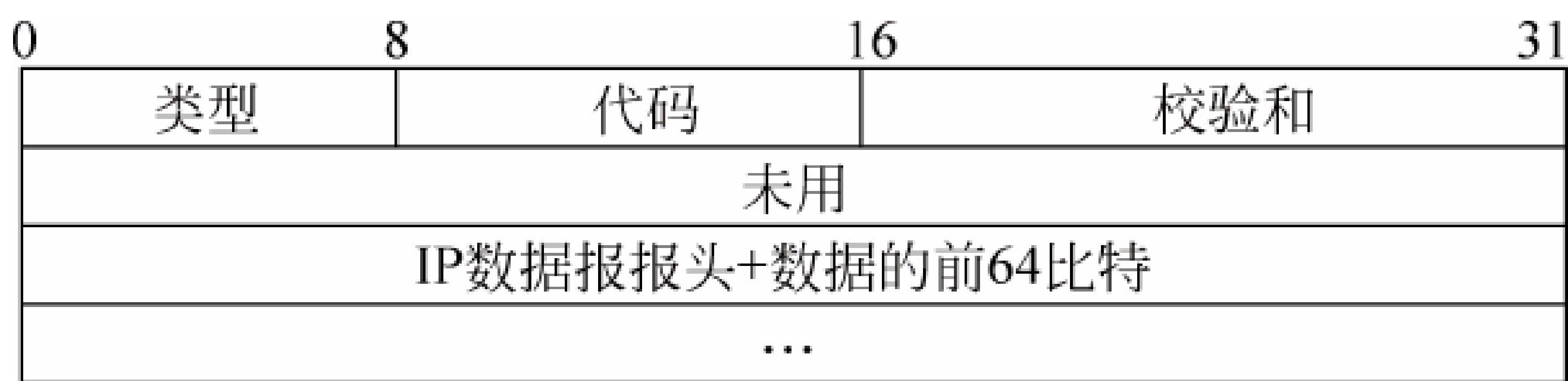



图 5-16　ICMP 目的地不可到达报文格式

ICMP 目的地不可到达报文根据代码值的不同，意义也不相同，大致可以分为几种类型，见表 5-4。

校验和由 16 位数据的反码和再取反而得，未计算校验和，该字段为 0，以后会被校验和取代。数据报报头＋64 位源数据报用于主机匹配信息到相应的进程。若高层协议使用端口号，应假定其在源数据的前 64 字节。

表 5-4　ICMP 目的地不可到达报文类型

| 码　值 | 意　　义 |
|---|---|
| 0 | 网络不可达 |
| 1 | 主机不可达 |
| 2 | 协议不可用 |
| 3 | 端口不可达 |
| 4 | 需要段和 DF 设置 |
| 5 | 源路由失败 |

**2. 超时报文**

网络的数据传送过程非常复杂，每个路由器都会独立地为 IP 数据报选路。一个路由器的路由选择出现问题，IP 数据报的传输就有可能出现死循环的情况，这就势必造成网络拥堵。但是可以利用 IP 数据报报头的生存周期字段有效地避免 IP 数据报在互联网中无休止地循环传输。超时的情况有以下几种。

（1）当路由器将一个数据报的生存时间字段的值随着时间减少为 0 时，路由器会放弃该数据报并发送一个超时报文。

（2）根据网络使用的技术不同，每种网络都规定了一个帧最多能够携带的数据量，这一限制称为最大传输单元（Maximum Transmission Unit，MTU）。因此，一个 IP 数据报的长度只有小于或等于一个网络的 MTU，才能在这个网络中传输。但如果一个 IP 数据报的长

度大于 MTU 时，就需要对此数据报进行分片，在各个分片到达目的地时，再进行重组，以保证 IP 数据报的完整。到一台主机对某一个数据报的重组时间截止，而此时该数据报的分片还没有全部到达，则主机放弃分片并发送一个超时报文。

ICMP 超时报文格式如图 5-17 所示。

ICMP 超时报文分为两种类型，见表 5-5。

| 0　　　　8 | 16 | 31 |
|---|---|---|
| 类型(11) | 代码(0～1) | 校验和 |
| 未用 | | |
| IP数据报报头+数据的前64比特 | | |
| … | | |

图 5-17　ICMP 超时报文格式

**表 5-5　ICMP 超时报文类型**

| 码　值 | 意　　义 |
|---|---|
| 0 | 传送超时 |
| 1 | 分段超时 |

**3. 参数出错报文**

参数出错报文主要用来报告错误的 IP 数据报报头和错误的 IP 数据报选项参数等情况。一旦参数错误严重到机器不得不抛弃 IP 数据报时，网关或主机便向源主机发送此报文，指出可能出现错误的参数位置。

## 5.4.3　ICMP 控制报文

ICMP 控制报文主要包括拥塞控制与源抑制报文和路由控制与重定向报文。

**1. 拥塞控制与源抑制报文**

所谓拥塞控制报文就是指遇到网络“拥塞”情况需要发送的报文。那么什么是“拥塞”呢？“拥塞”就是指 IP 数据报大量涌入到路由器的现象。造成“拥塞”的原因有以下两种。

(1) IP 数据报流入路由器的速度大于路由器流出 IP 数据报(转发 IP 数据报)速度的时候，IP 数据报就会拥堵在路由器内，造成“拥塞”。

(2) 路由器的处理速度过慢，使得流入到路由器的 IP 数据报排队，导致“拥塞”。无论造成拥塞的原因如何，都会影响网络的数据传输，因此，一定要想方设法来控制拥塞。目前主要采用的是“源站抑制”技术，即抑制源主机发送数据报的速率。具体的过程如下。

① 当路由器由于缺乏缓冲区空间而无法再接收数据报时，那么就抛弃新接收的 IP 数据报。每抛弃一个 IP 数据报，路由器便向该 IP 数据报的源主机发送一个 ICMP 源抑制报文。

② 为路由器的输出设置一个阈值，一旦路由器的数据报累积到一定的数量，超过这个阈值之后，如果再有新的 IP 数据报到来，路由器就主动向数据报的发送方发送 ICMP 源抑制控制报文。当源主机收到源抑制报文后，就会降低发送 IP 数据报的速度，直到不再收到源抑制报文为止。然后再恢复发送 IP 数据报的速度，直到再一次收到源抑制报文，形成一个良性的循环。

**2. 路由控制与重定向报文**

当路由器检测到一台源主机发送数据报选择的路由不是最优路径时，就会向该主机发送一个重定向 ICMP 报文，请这台源主机改变路由重新选择路径并把初始数据报转发给目的主机。重定向功能提供了一种路由优化控制机制，使源主机能以动态方式寻找最优路径。ICMP 路径重定向报文格式如图 5-18。

路由器的 IP 地址是指发往目的主机的最优路径中的第一个路由器地址，目的地地址由数据报报头中的目的地址字段表示。重定向报文分为 4 种类型，见表 5-6。

| 0 — 8 | 8 — 16 | 16 — 31 |
|---|---|---|
| 类型(5) | 代码(0～3) | 校验和 |
| 路由器IP地址 | | |
| IP数据报报头+数据的前64比特 | | |
| … | | |

图 5-18 ICMP 重定向报文格式

表 5-6 ICMP 重定向报文类型

| 码 值 | 意 义 |
|---|---|
| 0 | 重定向网络 |
| 1 | 重定向主机 |
| 2 | 重定向服务类型和网络 |
| 3 | 重定向服务类型和主机 |

## 5.4.4 ICMP 请求/应答报文对

为了便于分析和查找网络故障和控制网络，ICMP 还设计了请求/应答报文对，获取网络的一些重要信息，它主要包括回应请求与应答报文、时间戳请求与应答报文和掩码请求与应答报文。

**1. 请求与应答报文**

请求与应答报文主要对于测试目的主机或者路由器的可达性，报文格式如图 5-17 所示。某主机向指定的目的 IP 地址主机发送一个回应的请求，其中包含一个任选的数据区，要求具有目的 IP 地址的主机或路由器回应。当目的主机或路由器收到请求后，发出相应的响应应答，其中包含请求报文中任选数据的拷贝。也就是说，如果主机成功地收到一个应答，说明数据报传输系统的响应部分工作正常。Ping 命令就是利用 ICMP 回应请求与应答报文来测试目的主机的可达到性。

**2. 时间戳请求与应答报文**

设计时间戳请求与应答报文是为了努力达到互联网上主机时钟的同步，但是这种时钟同步技术的能力还是有限的。时间戳请求与应答报文格式如图 5-19 所示。

| 0 — 8 | 8 — 16 | 16 — 31 |
|---|---|---|
| 类型(13或14) | 代码(0) | 校验和 |
| 标识符 | | 序列号 |
| 发起时间戳 | | |
| 接收时间戳 | | |
| 传送时间戳 | | |

图 5-19 ICMP 时间戳与请求应答报文格式

**3. 掩码请求与应答报文**

掩码请求与应答报文主要用于源节点获取所在网络的 IP 地址掩码信息。源节点在发送请求报文时，将 IP 报头中的源 IP 地址和目的 IP 地址字段的网络号部分设为“0”。这样目的网络中的路由器接收到该请求时，将把网络的掩码向源节点回送应答报文。

# 思考与练习

## 一、填空题

1. ICMP 协议在网络中起到了差错控制和交通控制的作用。如果在 IP 数据报的传送过程中，如果出现网络拥塞，则路由器发出________报文。（国家软考网络工程师 2008 年试题）

2. ARP 协议数据单元封装在________中发送，ICMP 协议数据单元封装在________中发送。（国家软考网络工程师 2008 年试题）

## 二、选择题

1. ARP 协议的作用是 IP 地址求 MAC 地址，ARP 请求是广播发送，ARP 响应是（　　）发送。（国家软考网络工程师 2008 年试题）

A. 单播　　B. 组播　　C. 广播

2. 某公司网络的地址是 133.10.128.0/17，被划分成 16 个子网，下面的选项中不属于这 16 个子网的地址是（　　）。（国家软考网络工程师 2009 年试题）

A. 133.10.136.0/21　　B. 133.10.162.0/21

C. 133.10.208.0/21　　D. 133.10.224.0/21

3. IPv6 地址 12AB：0000：0000：CD30：0000：0000：0000：0000/60 可以表示成各种简写形式，下面的选项中，写法正确的是（　　）。

A. 12AB：0：0：CD30：：/60　　B. 12AB：0：0：CD3：：/60

C. 12AB：：CD30/60　　D. 12AB：：CD3/60

## 三、网络设计题

有 A、B、C 三个网络，每个网络的主机数分别是 20 台，25 台和 10 台主机，并用两个路由器 R1 和 R2 把它们互连起来，该网络的 IP 地址设定为 194.65.78.0。请为该互联网设计一个 IP 地址编址方案。

第6章

# 网络互联技术

## 6.1 网 络 互 联

所谓网络互联是指将两个以及两个以上的计算机网络，通过一定的方法，用一种或多种通信处理设备相互连接起来，以构成更大的网络系统。网络互联的形式有局域网与局域网、局域网与广域网、广域网与广域网的互联三种。是实现互相通信且共享软件、数据的系统。

## 6.2 网络互联设备

微型计算机的普及，导致了若干台微机相互连接，从而产生了局域网。由于网络的普遍应用，为了在更大范围内实现相互通信和资源共享，网络之间的互联便成为一种信息快速传递的最好方式。

网络互联时，必须解决如下问题：在物理上如何把两种或多种网络连接起来；一种网络如何与其他网络实现互访与通信；如何解决它们之间协议方面的差别；如何处理速率与带宽的差别。解决这些问题，协调、转换机制的部件就是网卡、中继器、集线器、网桥、交换机、路由器等网络互联设备。

### 6.2.1 网卡

网络适配器又称网卡或网络接口卡(Network Interface Card，NIC)。它是使计算机联网的设备。平常所说的网卡就是将PC和LAN连接的网络适配器。网卡插在计算机主板插槽中，负责将用户要传递的数据转换为网络上其他设备能够识别的格式，通过网络介质传输。它的主要技术参数为带宽、总线方式、电气接口方式等。它的基本功能为从并行到串行的数据转换，包的装配和拆装，网络存取控制，数据缓存和网络信号。目前主要是8位和16位网卡。

网卡必须具备两大技术：网卡驱动程序和I/O技术。驱动程序使网卡和网络操作系统兼容，实现PC与网络的通信。I/O技术可以通过数据总线实现PC和网卡之间的通信。网卡是计算机网络中最基本的元素。在计算机局域网络中，如果有一台计算机没有网卡，那么这台计算机将不能和其他计算机通信，也就是说，这台计算机在网络中是孤立的。

网卡的不同分类：根据网络技术的不同，网卡的分类也有所不同，如ATM网卡、令牌环网卡和以太网网卡等。据统计，目前约有80%的局域网采用以太网技术。就兼容网卡而言，目前，网卡一般分为普通工作站网卡和服务器专用网卡。服务器专用网卡是为了适应网络服务种类较多，性能也有差异，它可按以下的标准进行分类：按网卡所支持带宽的不同可分为10Mb/s网卡、100Mb/s网卡、10/100Mb/s自适应网卡、1000Mb/s网卡几种；根据网卡总线类型的不同，主要分为ISA网卡、EISA网卡和PCI网卡三大类，其中ISA网卡和PCI网卡较常使用。ISA总线网卡的带宽一般为10Mb/s，PCI总线网卡的带宽从10Mb/s到1000Mb/s都有。同样是10Mb/s网卡，因为ISA总线为16位，而PCI总线为32位，所以PCI网卡要比ISA网卡快。

网卡的接口类型：根据传输介质的不同，网卡出现了AUI接口(粗缆接口)、BNC接口(细缆接口)和RJ-45接口(双绞线接口)三种接口类型。市面上常见的10Mb/s网卡主要有单口网卡(RJ-45接口或BNC接口)和双口网卡(RJ-45和BNC两种接口)，带有AUI粗缆接口的网卡较少。而100Mb/s和1000Mb/s网卡一般为单口卡(RJ-45接口)。

### 6.2.2 中继器

中继器(Repeater)是网络物理层上面的连接设备。适用于完全相同的两类网络的互联，主要功能是通过对数据信号的重新发送或者转发，来扩大网络传输的距离。中继器是对信号进行再生和还原的网络设备，工作在OSI模型的物理层。

中继器是连接网络线路的一种装置，常用于两个网络节点之间物理信号的双向转发工作。中继器是最简单的网络互联设备，主要完成物理层的功能，负责在两个节点的物理层上按位传递信息，完成信号的复制、调整和放大功能，以此来延长网络的长度。由于存在损耗，在线路上传输的信号功率会逐渐衰减，衰减到一定程度时将造成信号失真，因此会导致接收错误。中继器就是为解决这一问题而设计的。一般情况下，中继器的两端连接的是相同的媒体，但有的中继器也可以完成不同媒体的转接工作。从理论上讲中继器的使用是无限的，网络也因此可以无限延长。事实上这是不可能的，因为网络标准中都对信号的延迟范围做了具体的规定，中继器只能在此规定范围内进行有效的工作，否则会引起网络故障。连接同一个网络的两个或多个网段，如以太网常常利用中继器扩展总线的电缆长度，标准细缆以太网的每段长度最大185米，最多可有5段，因此增加中继器后，最大网络电缆长度则可提高到925米。一般来说，中继器两端的网络部分是网段，而不是子网。因此中继器的优点主要包括了扩大了通信距离，但代价是增加了一些存储转发延时；增加了节点的最大数目；各个网段可使用不同的通信速率；提高了可靠性。当网络出现故障时，一般只影响个别网段；性能得到改善。当然，使用中继器也有一定的缺点，例如由于中继器对收到被衰减的信号再生(恢复)到发送时的状态，并转发出去，增加了延时；CAN总线的MAC子层并没有流量控制功能。当网络上的负荷很重时，可能因中继器中缓冲区的存储空间不够而发生溢出，以致产生帧丢失的现象；中继器若出现故障，对相邻两个子网的工作都将产生影响。

### 6.2.3 集线器

集线器的英文称为“Hub”。“Hub”是“中心”的意思,集线器的主要功能是对接收到的信号进行再生整形放大,以扩大网络的传输距离,同时把所有节点集中在以它为中心的节点上。它工作于OSI参考模型的物理层。集线器与网卡、网线等传输介质一样,属于局域网中的基础设备,采用CSMA/CD访问方式。集线器属于纯硬件网络底层设备,基本上不具有类似于交换机的“智能记忆”能力和“学习”能力,采用广播方式发送数据。这种广播发送数据方式有三方面不足:

(1) 用户数据包向所有节点发送,很可能带来数据通信的不安全因素,一些别有用心的人很容易就能非法截获他人的数据包。

(2) 由于所有数据包都是向所有节点同时发送,可能造成网络塞车现象,更加降低了网络执行效率。

(3) 非双工传输,网络通信效率低。集线器的同一时刻每一个端口只能进行一个方向的数据通信,而不能像交换机那样进行双向双工传输,网络执行效率低,不能满足较大型网络通信需求。

正因如此,尽管集线器技术也在不断改进,但实质上就是加入了一些交换机(Switch)技术,发展到了今天的具有堆叠技术的堆叠式集线器,有的集线器还具有智能交换机功能。可以说集线器产品已在技术上向交换机技术进行了过渡,具备了一定的智能性和数据交换能力。但随着交换机价格的不断下降,仅有的价格优势已不再明显,集线器的市场越来越小,处于被淘汰的边缘。尽管如此,集线器对于家庭或者小型企业来说,在经济上还是有一点诱惑力的,特别适合家庭几台机器的网络中或者中小型公司作为分支网络使用。

### 6.2.4 网桥

网桥(Bridge)像一个聪明的中继器。中继器从一个网络电缆里接收信号,放大它们,将其送入下一个电缆。相比较而言,网桥对从网卡上传下来的信息更敏锐一些。网桥是一种对帧进行转发的技术,根据MAC分区块,可隔离碰撞。网桥将网络的多个网段在数据链路层连接起来。它工作于数据链路层,不但能扩展网络的距离或范围,而且可提高网络的性能、可靠性和安全性。网络1和网络2通过网桥连接后,网桥接收网络1发送的数据包,检查数据包中的地址,如果地址属于网络1,它就将其放弃,相反,如果是网络2的地址,它就继续发送给网络2。这样可利用网桥隔离信息,将同一个网络号划分成多个网段(属于同一个网络号),隔离出安全网段,防止其他网段内的用户非法访问。由于网络的分段,各网段相对独立,一个网段的故障不会影响到另一个网段的运行。

网桥的基本特征包括网桥在数据链路层上实现局域网互联;能够互联两个采用不同数据链路层协议、不同传输介质与不同传输速率的网络;网桥以接收、存储、地址过滤与转发的方式实现互联的网络之间的通信;网桥需要互联的网络在数据链路层以上采用相同的协

议；网桥可以分隔两个网络之间的通信量，有利于改善互联网络的性能与安全性。

网桥的存储和转发功能与中继器相比有优点也有缺点。其优点是：使用网桥进行互联克服了物理限制，这意味着构成 LAN 的数据站总数和网段数很容易扩充；网桥纳入存储和转发功能可使其适应于连接使用不同 MAC 协议的两个 LAN，因而构成一个不同 LAN 混连在一起的混合网络环境；网桥的中继功能仅仅依赖于 MAC 帧的地址，因而对高层协议完全透明；网桥将一个较大的 LAN 分成段，有利于改善可靠性、可用性和安全性。网桥的主要缺点是：由于网桥在执行转发前先接收帧并进行缓冲，与中继器相比会引入更多时延；由于网桥不提供流控功能，因此在流量较大时有可能使其过载，从而造成帧的丢失。网桥的优点多于缺点正是其广泛使用的原因。

网桥工作在数据链路层，将两个 LAN 连起来，根据 MAC 地址来转发帧，可以看作一个“低层的路由器”（路由器工作在网络层，根据网络地址如 IP 地址进行转发）。

远程网桥通过一个通常较慢的链路（如电话线）连接两个远程 LAN，对本地网桥而言，性能比较重要，而对远程网桥而言，在长距离上可正常运行是更重要的。

### 6.2.5　交换机

交换（Switching）是按照通信两端传输信息的需要，用人工或设备自动完成的方法，把要传输的信息送到符合要求的相应路由上的技术的统称。广义的交换机（Switch）就是一种在通信系统中完成信息交换功能的设备。交换机主要具有地址学习、帧的转发和过滤等功能。

在计算机网络系统中，交换概念的提出改进了共享工作模式。Hub 集线器就是一种共享设备，Hub 本身不能识别目的地址，当同一局域网内的 A 主机给 B 主机传输数据时，数据包在以 Hub 为架构的网络上是以广播方式传输的，由每一台终端通过验证数据包头的地址信息来确定是否接收。也就是说，在这种工作方式下，同一时刻网络上只能传输一组数据帧的通讯，如果发生碰撞还得重试。这种方式就是共享网络带宽。与集线器不同，交换机能够根据网络中不同主机上网卡的 MAC 地址直接对目的节点发送数据包，这种方式明显比 Hub 的广播式传输效率要高；对于 Hub 来说，所有连接在 Hub 上的节点都处在同一个冲突域中，而对于交换机来说，一个端口就是一个冲突域。

和网桥比较，交换机实质上就是一个多端口的网桥，它是多个网桥功能的集合，在传输速率上交换机要高于网桥；在 MAC 地址的学习上，交换机更为主动，它会向所有端口发送广播帧，从回应帧中学习到不同主机的 MAC 地址，建立自己的 MAC 地址与端口对应关系表。

### 6.2.6　路由器

路由器（Router）是连接因特网中各局域网、广域网的设备，它接收到其他节点发送来的数据包后，会根据数据包中的源 IP 地址和目的 IP 地址，查找缓存中的路由表，根据信道的

情况，找出一条最佳、最经济、最快捷的路径，把数据包发送到目的节点，也就是我们常说的路由选择；目前，互联网中存在着不同通信协议的网络，比如 TCP/IP 协议、IPX/SPX 协议等，因此路由器还具有不同网络之间的协议转换功能；同时路由器还具有拥塞控制、安全保护等功能。

路由器和交换机是两种不同的网络设备，它们之间的主要区别就是交换发生在 OSI 参考模型数据链路层，而路由发生在网络层。这一区别决定了路由和交换在传输信息的过程中依据的对象不同，交换机依据数据帧中的 MAC 地址来转发数据，路由器则依据数据包中的 IP 地址来转发数据。交换机处理的信息单元是数据帧，而路由器处理的数据单元是数据包。传统交换机的每一个端口为一个冲突域，缩小了冲突范围，但它转发广播包，所以交换机的所有端口在一个广播域，而路由器不转发广播包，可以分割广播域。

## 6.3 路由器和路由选择

路由器是连接多个网络的互联设备，路由器一般至少连接两个网络，并根据具体协议选择每个数据包的传输路径。

路由器实际上就是一台特殊的计算机，也是由硬件和软件组成的，目前路由器已经广泛应用于各行各业，各种不同档次的产品已成为实现各种骨干网内部连接、骨干网间互联和骨干网与互联网互联互通业务的主力军。

本节先介绍路由器的硬件组成和软件组成，重点要掌握的是路由器的软件 IOS，因为对路由器的配置即是对 IOS 的配置，IOS 内部提供了大量的命令供我们使用，熟悉这些命令才可以发挥路由器的功能，本节介绍的是路由器最基础的命令。

### 6.3.1 路由器的硬件组成

路由器的硬件组成如下。

**1. 中央处理器(CPU)**

与计算机一样，路由器也包含了一个中央处理器(Central Processing Unit，CPU)。不同系列和型号的路由器，其中的 CPU 也不尽相同。路由器的 CPU 负责路由器的配置管理和数据包的转发工作，如维护路由器所需的各种表格以及路由运算等。路由器对数据包的处理速度很大程度上取决于 CPU 的类型和性能。

**2. 内存**

路由器采用了以下几种不同类型的内存，每种内存以不同方式协助路由器工作。

(1) 只读内存(Read-Only Memory，ROM)：只读内存在路由器中的功能与计算机中的 ROM 相似，只能读取而不能写入，通常用来存储生产厂家固化写入的程序数据，在特定专业条件下才可以写入如要进行升级，则要替换 ROM 芯片。

(2) 闪存(Flash)：闪存是可读可写的存储器，在系统重新启动或关机之后仍能保存数

据。Flash 中存放着当前使用中的 IOS。事实上，如果 Flash 容量足够大，甚至可以存放多个操作系统，这在进行 IOS 升级时十分有用。当不知道新版 IOS 是否稳定时，可在升级后仍保留旧版 IOS，当出现问题时可迅速退回到旧版操作系统，从而避免长时间的网路故障。

（3）非易失性 RAM（Non-Volatile Random Access Memory，NVRAM）：非易失性 RAM 是可读可写的存储器，在系统重新启动或关机之后仍能保存数据。由于 NVRAM 仅用于保存启动配置文件（Startup-Config），故其容量较小，通常在路由器上只配置 32～128KB 大小的 NVRAM。同时，NVRAM 的速度较快，成本也比较高。

（4）随机存储器（Random Access Memory，RAM）：RAM 也是可读可写的存储器，但它存储的内容在系统重启或关机后将被清除。和计算机中的 RAM 一样，路由器中的 RAM 也是运行期间暂时存放操作系统和数据的存储器，让路由器能迅速访问这些信息。RAM 的存取速度优于前面所提到的 3 种内存的存取速度。

运行期间，RAM 中包含路由表项目、ARP 缓冲项目、日志项目和队列中排队等待发送的分组。除此之外，还包括运行配置文件（Running-Config）、正在执行的代码、IOS 操作系统程序和一些临时数据信息。

图 6-1 为路由器硬件面板结构图。

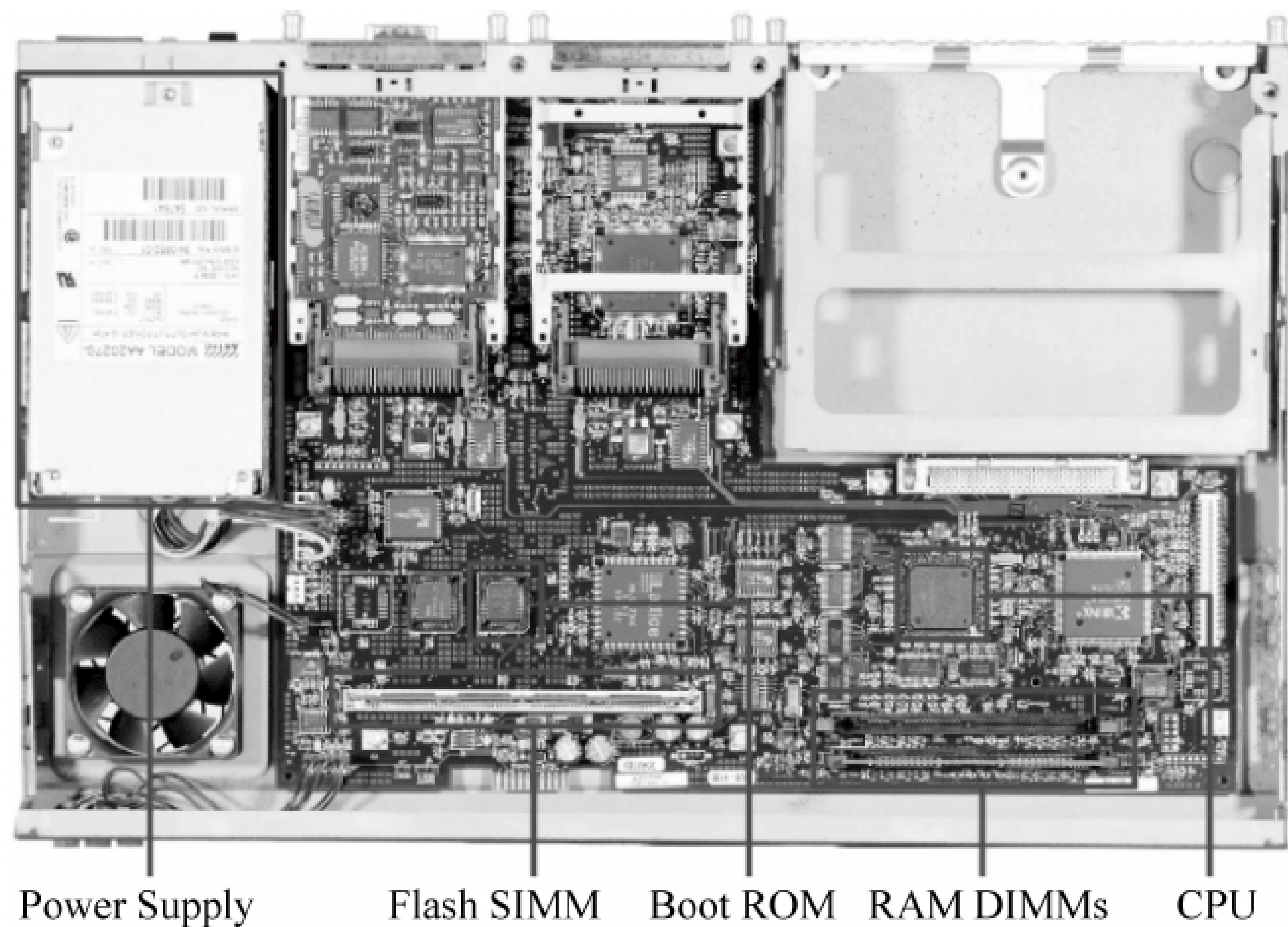



图 6-1　路由器硬件面板结构图

## 6.3.2　路由器加电启动过程

（1）系统硬件加电自检。运行 ROM 中的硬件检测程序，检测各组件能否正常工作。完成硬件检测后，开始软件初始化工作。

（2）软件初始化过程。运行 ROM 中的 BootStrap 程序，进行初步引导工作。

（3）寻找并载入 IOS 系统文件。IOS 系统文件可以存放在多处，至于到底采用哪一个

IOS,是通过命令设置指定的。

(4) IOS 装载完毕,系统在 NVRAM 中搜索保存的 Startup-Config 文件,进行系统的配置。如果 NVRAM 中存在 Startup-Config 文件,则将该文件调入 RAM 中并逐条执行。否则,系统进入 Setup 模式,进行路由器初始配置。

### 6.3.3 路由器接口

所有路由器都有接口(Interface),每个接口都有自己的名字和编号。一个接口的全名由它的类型标志与数字编号构成,编号自 0 开始。对于接口固定的路由器(如 Cisco 2500 系列)或采用模块化接口的路由器(如 Cisco 4700 系列),在接口的全名称中,只采用一个数字,并根据它们在路由器的物理顺序进行编号,例如 Ethernet0 表示第 1 个以太网接口,Serial1 表示第 2 个串口。FastEthernet 0/0 第一个 0 代表槽位号,也就是模块化路由器的扩展槽,后面的 0 代表第一个快速以太网口,Serial0/0/0 第一个 0 代表槽位号,第二个 0 代表多业务卡的编号,最后面的 0 代表多业务卡上的第一个接口。

控制台端口:所有路由器都安装了控制台端口,使用户或管理员能够利用终端与路由器进行通信,完成路由器配置。该端口提供了一个 EIA/TIA-232 异步串行接口,用于在本地对路由器进行配置(首次配置必须通过控制台端口进行)。如图 6-2 为路由器背板面板接口。

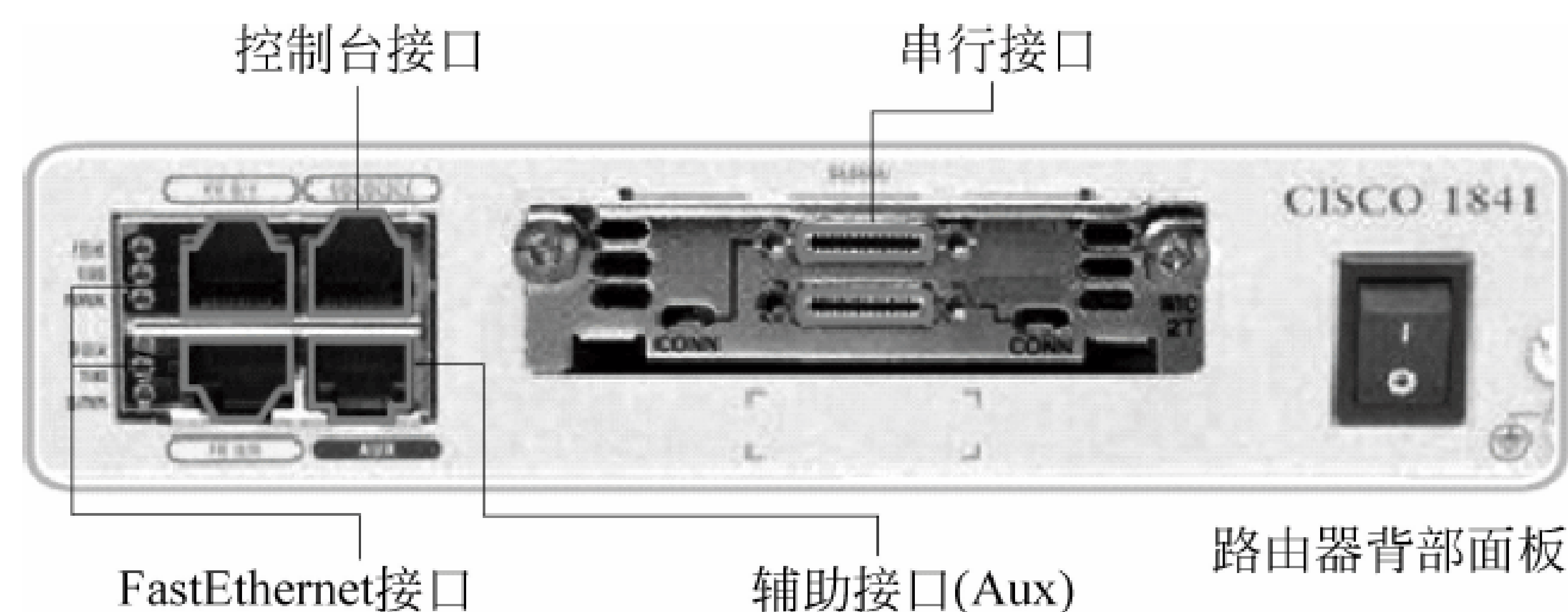



图 6-2 路由器背板面板接口

Aux 接口:这是"Auxiliary(辅助)"的缩写,主要用于远程配置,也可用于拨号连接,还可通过收发器与 Modem 进行连接。

### 6.3.4 路由器的软件组成

和 PC 相同,路由器也需要操作系统才能运行。IOS(Internet Operation System Software)是 Cisco System 公司跨越主要路由和交换产品的软件平台,提供路由器所有的核心功能。

### 6.3.5 路由选择

由前面的叙述可知,路由器主要有两个方面的基本功能。

（1）寻找一条到达目的网络的最佳路径。

（2）将分组从一个接口传递到另一个接口，从而将分组传递到接收站。

为了完成以上两个功能路由器需要做以下工作。

（1）学习周围与其相连的路由器，从而确定可以到达的网络。

（2）选择到每个目的网络的最佳路径。

（3）维护关于如何到达目的网络的最新路由选择信息。

（4）转发数据时，检查入站的 IP 分组中的目的 IP 地址、确定目的网络号、查看路由选择表并将分组转发到出站口。

要理解路由器是怎样完成这些工作的，就需要了解路由选择协议以及路由器如何使用它们。

**1．路由简介**

路由器的路由表有两种生成方法：一是用手工配置路由表，二是由路由器自动生成路由表。按照路由表项目的生成方法，可把路由分为 3 类，直连路由、静态路由和动态路由。

（1）直连路由：直连路由就是与路由器直接相连的网络。这种路由在我们配置好路由器的各个接口时就自动生成了。所以我们可以认为路由器可自动识别与它直接相连的各个网络。

（2）静态路由：这是一种由网管手工配置的路由路径。网管必须了解路由器的拓扑连接，通过手工方式指定路由路径，而且在网络拓扑发生变动时，也需要网管手工修改路由路径。

（3）动态路由：动态路由是一种通过某种路由协议，由路由器自学到的路由，它不需要手工配置路由表，而且当网络的拓扑结构发生变化，路由器会重新计算路由，自动更新路由表，不需人工干预，特别适合大范围网络的路由。

**2．动态路由选择协议**

动态路由是由路由器自学后，自动生成路由表，自动进行路由的选择。路由器是如何自学，又是如何选择路由的呢？我们需要了解动态路由选择协议。

动态路由选择协议可以分为三类：距离向量协议、链路状态协议和混合协议。每种路由选择协议都是有区别的，各有优缺点，选择路由选择协议需要考虑以下因素。

- 用于选择路径的路由选择度量值。
- 路由选择信息如何共享。
- 路由选择协议的收敛速度。
- 路由器如何处理路由选择信息。
- 路由选择协议的开销。

路由选择的度量值是多方面的，比如有带宽（以 Kb/s 计）、成本（与链路的带宽成反比）、延迟、跳数、负载、最大传输单元以及可靠性等。

路由选择信息的共享方式有：广播、组播和单播。

收敛是指所有路由器了解当前网络拓扑所花的时间。距离向量协议趋向于缓慢收敛，而链路状态协议趋向于迅速收敛。

1）距离向量协议

在动态路由选择协议中距离向量协议是最简单的，用距离（如 RIP 中的跳数）和方向（向量）来寻找到达目的网络的路径。RIP 就属于距离向量协议。

距离向量协议使用目的 IP 地址 255.255.255.255 周期性地广播路由选择信息，不管有没有变化都坚持这么做，一旦周期计时器期满，它们就向连接在其接口上的任何设备广播其路由选择信息。运行距离向量协议的路由器通过收听路由选择广播来学习其邻居。学习到路由更新信息后，路由器更新自己的路由表，并且把从邻居路由器得来的路由选择信息又以广播的形式发布出去，所以这种协议又被称为传闻路由选择。距离向量协议是三类协议当中最简单的，易于设置和排除故障，开销极低。

2）链路状态协议

链路状态协议使用最短路径优先（Shortest Path Fivst，SPF）算法来寻找到达接收站的最佳路径。链路状态协议学习网络的完整拓扑：哪些路由器连接到哪些网络。由于网络的尺寸，这会造成可扩展性问题。因此，链路状态协议通常具有限制其学习进程的范围，将路由器对网络拓扑的知识限制到更少的路由器。链路状态协议有 OSPF、IS-IS。

距离向量协议周期性地广播路由选择信息，占用了网络带宽，并且不需要对广播进行确认。而链路状态协议仅在网络发生变化时以组播的形式发送链路状态通告（Link-State Advertisement，LSA），接收路由器还要予以确认，链路状态协议也不会生成路由选择环路。所以它比距离向量协议更能高效地使用网络带宽和资源，但它更耗费路由器的 CPU 和内存资源。

3）混合协议

混合协议采用了距离向量协议和链路状态协议的优点，将它们合成为一种新的协议。通常，混合协议是基于距离向量协议，但具有链路状态协议的很多特点和优点。混合协议的例子有 RIPv2、EIGRP 和 BGP。

过去对于中小网络来说，距离向量协议（如 RIP）运行的较多，随着硬件的发展，距离向量协议很少使用了，而链路状态协议用得多起来，尤其是 OSPF，而在 SOHO 网络中，静态路由是最常用的路由选择机制。

## 6.4 路由器的配置

### 6.4.1 路由器的基本配置

Cisco 路由器可以通过 5 种方式来进行配置，如图 6-3 所示。

（1）通过 Console 口访问路由器。新的路由器第一次配置时必须通过 Console 接口访

问路由器。

（2）通过 Telnet 访问路由器。

（3）通过终端访问服务器。

（4）通过 Aux 接口接 Modem 访问路由器。

（5）通过 Ethernet 上的 SNMP 网管工作站。

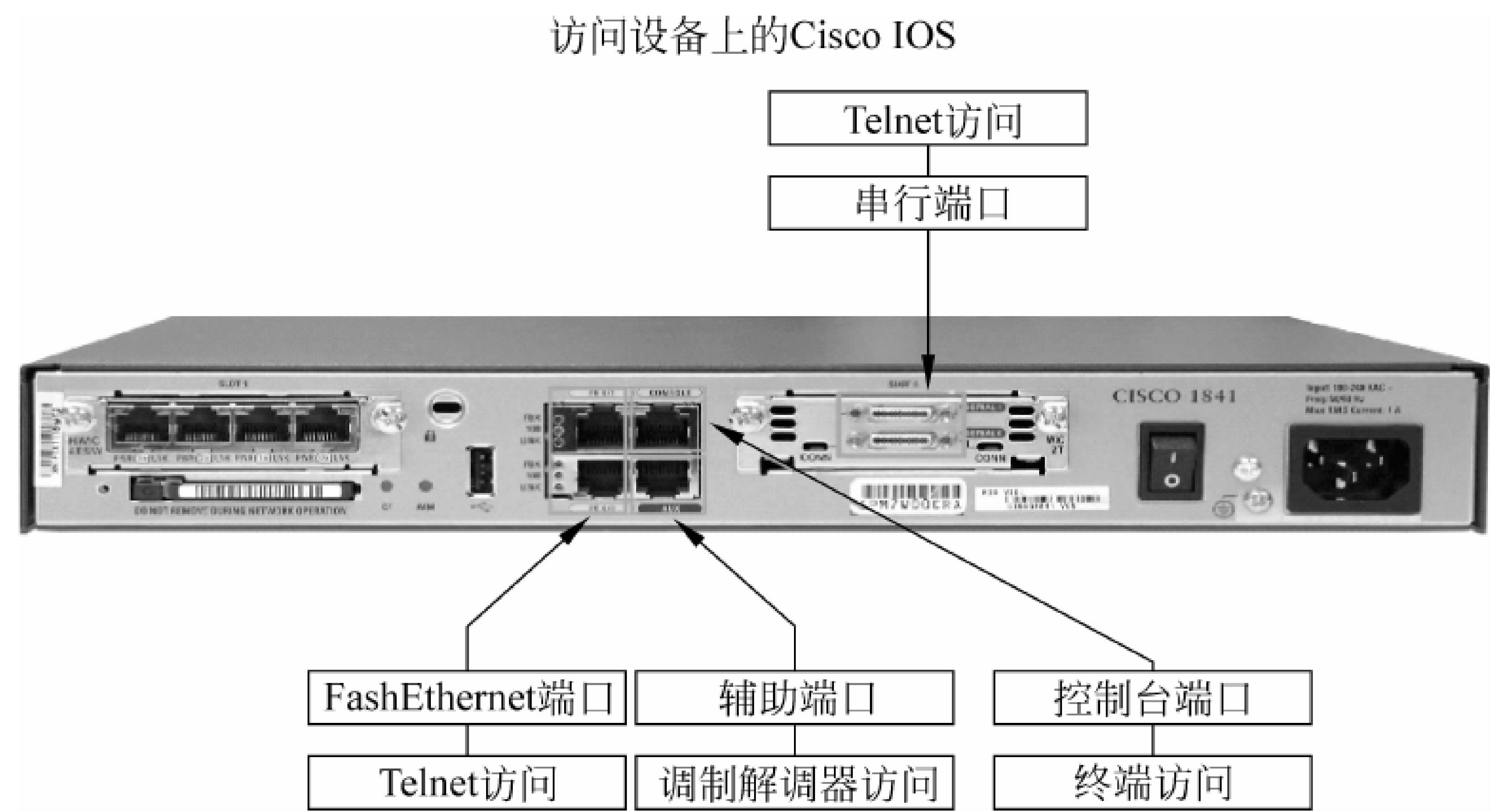



图 6-3　路由器各种访问端口

在这里以 Console 口访问和 Telnet 访问为例进行详细介绍。

通过 Console 口访问路由器。这是一种最常用的访问路由器的方式，计算机的串口和路由器的 Console 口是通过反转线（Roll Over）进行连接的，反转线的一端接在路由器的 Console 口上，另一端接到一个 DB9-RJ45 的转接头上，DB9 则接到计算机的串口上。所谓的反转线就是线两端的 RJ45 接头上的线序正好相反，如图 6-4 所示。

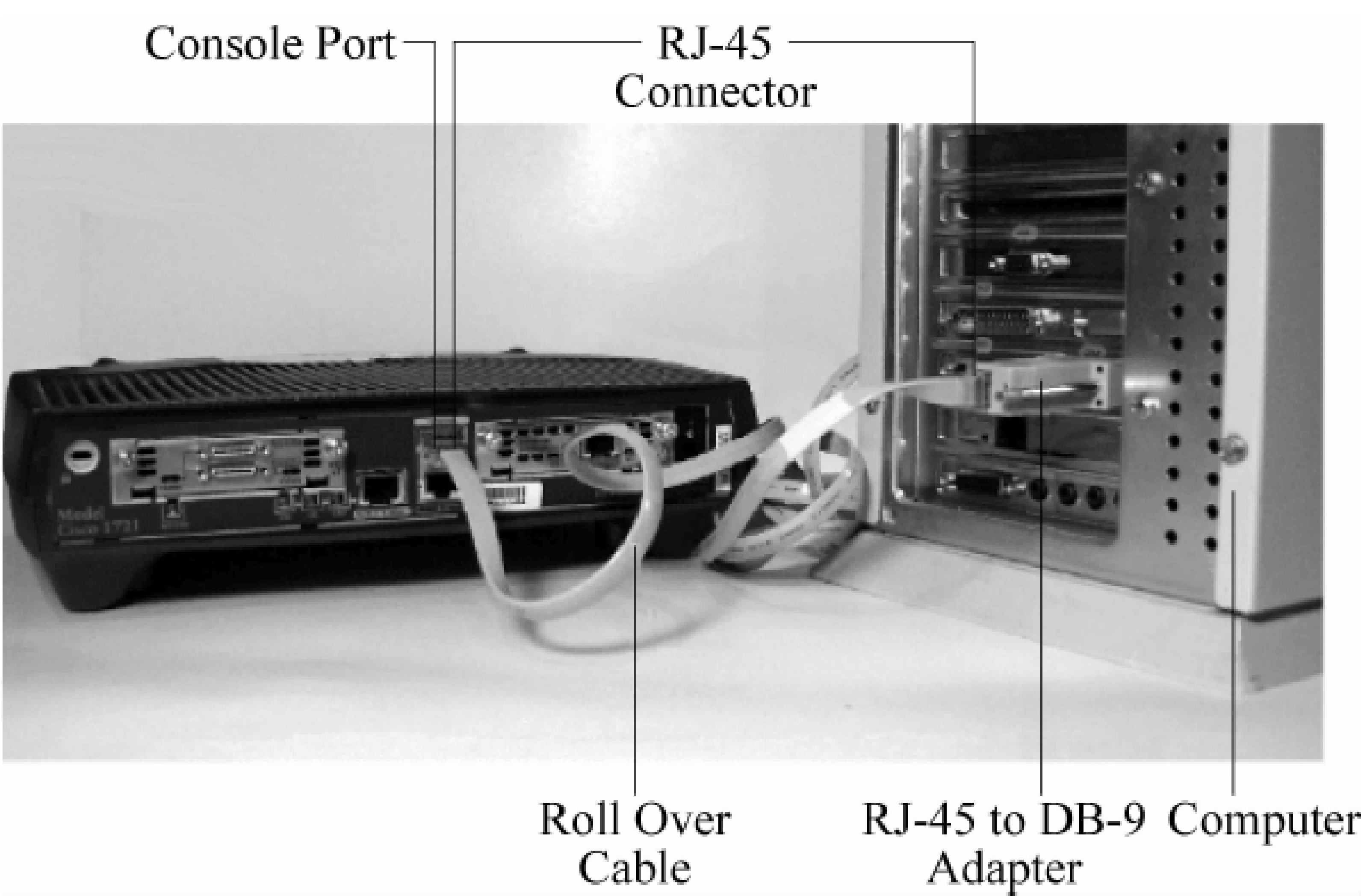



图 6-4　路由器访问接口

计算机和路由器连接好后，可以使用各种各样的终端软件配置路由器了。

通过 Telnet 访问路由器。除了首次配置以外，这应该是最常用的路由器访问方式了，因为在有多台路由器的情况下，不可能每次操作都接到 Console 口，当然这需要预先在路由器上配置 IP 地址和密码，并保证管理员的计算机和路由器之间是 IP 可达的（简单讲就是能 Ping 通）。Cisco 路由器通常支持多人同时 Telnet，每一个用户称为一个虚拟终端（VTY）。第一个用户为 VTY 0，第二个用户为 VTY 1，依次类推，路由器通常到 VTY 4。

Cisco IOS CLI 操作：路由器的用户接口被称为命令行接口（Command-Line Interface，CLI）。CLI 是基于命令行格式，CLI 让用户通过键盘输入命令，路由器在用户的屏幕上返回一系列文本信息。路由器没有显示器和键盘，所以 IOS CLI 需要借助于计算机的显示器和键盘并且保证计算机和路由器的物理连接正常通信。

路由器的工作模式：

**1. 用户模式：router>**

路由器处于用户命令状态，这时用户可以看路由器的连接状态，访问其他网络和主机，但不能看到和更改路由器的设置内容。

**2. 特权模式：router#**

在 router>提示符下输入 enable，路由器进入特权命令状态 router#，这时不但可以执行所有的用户命令，还可以看到和更改路由器的设置内容，主要 show 命令在此模式下。

使用 exit 退回至 router>。

**3. 全局配置模式：router(config)#**

在 router#提示符下输入 configure terminal，出现提示 router(config)#，此时路由器处于全局设置状态，这时可以设置路由器的全局参数。可以配置主机名等全局命令。

使用 exit、end 或 Ctrl+Z 退回至 router#。

**4. 子配置模式：router(config-if)#**

router(config-line)#

router(config-router)#

路由器处于局部设置状态，这时可以设置路由器某个局部的参数。具体配置在此模式下进行，比如接口配置、路由配置等。

使用 exit 退回至 router(config)#。

使用 end、Ctrl+Z 退回至 router#。

enable 和 disable 命令用于使 CLI 在用户模式和特权模式。

在任何配置模式下或配置子模式下输入 exit 命令，则返回上一级模式。在用户模式下输入 exit 则完全退出路由器。

### 6.4.2 静态路由的配置

静态路由是非常广泛、稳定、并且简单的路由协议，不存在动态路由协议的收敛过程。缺点是在大型网络中，配置的工作量非常大，特别是网络拓扑改变时需要作大量配置修改，所以静态一般作为动态路由协议的补充。

默认静态路由是一种特殊的静态路由，用来指明一些下一跳没有明确列于路由表中的数据包应如何转发。对于在路由表中找不到明确路由条目的所有的数据包，都将按照默认静态路由指定的接口或下一跳地址进行转发。其优点是能够极大地减少路由表条目，缺点是不正确配置可能导致路由环路。

浮动静态路由有时也会使用，作用是对动态路由的补充，如果动态路由出现故障，该静态路由马上启用，优点是保证了网络的高可用性。

静态路由的配置方法如下。

```
Router(config)#ip route network mask {address|interface} [distance]
```

其中：

network　目标网络或子网地址。

mask　子网掩码。

address　下一跳的 IP 地址或相邻路由器的端口地址。

interface　相邻路由器的端口名称。

distance　管理距离。

静态路由的优点：

静态路由不会占用路由器的 CPU、RAM 等。静态路由需要网络管理员完全参与，并且对网络拓扑非常熟悉，当网络拓扑发生变化时，需要网络管理员手动修改路由信息。使用静态路由，网络安全保密性高。动态路由因为需要路由器之间频繁地交互各自的路由表，而对路由表的分析可以得到网络的拓扑结构和网络地址等信息。

静态路由的缺点：

大型和复杂的网络环境通常不适合采用静态路由。一方面，网络管理员难以全面地了解整个网络的拓扑结构；另一方面，当网络的拓扑结构和链路状态发生变化时，路由器中的静态路由信息需要大范围地调整，这一工作的难度和复杂程度非常高。

### 6.4.3 路由信息协议及其配置

动态路由协议包括距离向量路由协议和链路状态路由协议。路由信息协议（Routing Information Protocol，RIP）是使用最广泛的距离向量路由协议。

RIP 是由 Xerox 在 70 年代开发的路由协议。RIP 协议在目前已成为路由器、主机路由信息传递的标准协议之一，并被路由器厂商广泛使用。RIP 协议的设计初衷是用于中小型

网络，对于更大、更复杂的环境，一般不使用 RIP 协议。RIP 协议处于 UDP 协议的上层，RIP 所接收的路由信息都封装在 UDP 的数据报文中，RIP 在 UDP 的 520 端口上接收来自远程路由器的路由更新信息，并对本地的路由表做相应的修改，同时通知其他路由器。通过这种方式，达到全局路由的有效。RIP 协议分为 RIPv1 和 RIPv2 两个版本。

RIP 使用跳数(Hop Count)来衡量到达目的地址的距离，称为度量值。在 RIP 中，路由器到与它直接相连网络的跳数为 0，通过一个路由器可达的网络的跳数为 1，依此类推。RIP 规定度量值取 0～15 之间的整数，大于或等于 16 的跳数被定义为无穷大，即目的网络或主机不可达。由于这个限制，使得 RIP 不可能在大型网络中得到应用。

RIPv1 是有类别路由协议，它只支持以广播方式发布报文。RIPv1 的报文中没有携带掩码信息，它只能识别主类的路由，因此 RIPv1 无法支持路由聚合，也不支持不连续子网。

RIPv2 是一种无分类路由协议，与 RIPv1 相比，它有以下优势：

(1) 报文中携带掩码信息，支持路由聚合和 CIDR(Classless Inter-Domain Routing)。

(2) 支持组播路由发送更新报文，只有 RIPv2 路由器才能收到协议报文，减少资源消耗。

(3) 支持对协议报文进行验证，并提供明文验证和 MD5 验证两种方式，增强安全性。

RIP 的特点：仅和相邻的路由器交换信息。如果两个路由器之间的通信不经过任何路由器，那么这两个路由器是相邻的；路由器交换的信息是当前本路由器所知道的全部信息。即自己的整张路由表；每隔 30s 交换路由信息，然后路由器根据收到的路由信息更新自己的路由表。

RIP 路由配置常用命令解释如下。

router rip　指定使用 RIP 协议。

version {1/2}　指定 RIP 协议版本。

network　指定与该路由器直接相连的网络。

neighbor　指定需要定点传送的地址。

passive interface　阻止在指定的接口发送路由更新信息。

show ip route　查看路由表信息。

show route rip　查看 RIP 协议路由信息。

为提高性能，防止产生路由循环，RIP 的防环机制共有 5 种。

(1) 记数无穷大(Maximum Hop Count)：定义最大跳数(最大为 15 跳)，当跳数为 16 跳时，目标为不可达。

(2) 水平分割(Split Horizon)：从一个接口学习到的路由不会再广播回该接口。Cisco 可以对每个接口关闭水平分割功能。这个特点在非广播多路访问 Hub-And-Spoke 环境下十分有用。

(3) 毒性逆转(Poison Reverse)：从一个接口学习的路由会发送回该接口，但是已经被毒化，跳数设置为 16 跳，不可达。

（4）触发更新（Trigger Update）：一旦检测到路由崩溃，立即广播路由刷新报文，而不等到下一刷新周期。

（5）抑制计时器（Holddown Timer）：防止路由表频繁翻动，增加了网络的稳定性。

### 6.4.4　OSPF 协议及其配置

随着 Internet 技术在全球范围的飞速发展，OSPF 已成为目前 Internet 和 Intranet 采用最多、应用最广泛的路由协议之一。OSPF（Open Shortest Path First）路由协议是由 IETF（Internet Engineering Task Force）IGP 工作小组提出的，是一种基于 SPF 算法的路由协议，目前使用的 OSPF 协议是其第二版，定义于 RFC1247 和 RFC1583。

OSPF 作为一种内部网关协议（Interior Gateway Protocol，IGP），用于在同一个自治域（Autonomous System，AS）中的路由器之间发布路由信息。区别于距离矢量协议（RIP），OSPF 具有支持大型网络、路由收敛快、占用网络资源少等优点，在目前应用的路由协议中占有相当重要的地位。

基本概念和术语如下。

链路状态：OSPF 路由器收集其所在网络区域上各路由器的连接状态信息，即链路状态信息（Link-State，LS），生成链路状态数据库（Link-State Database，LSD）。路由器掌握了该区域上所有路由器的链路状态信息，也就等于了解了整个网络的拓扑状况。OSPF 路由器利用"最短路径优先算法（Shortest Path First，SPF）"，独立地计算出到达任意目的地的路由。

区域：OSPF 协议引入"分层路由"的概念，将网络分割成一个"主干"连接的一组相互独立的部分，这些相互独立的部分被称为"区域"（Area），"主干"的部分称为"主干区域"。每个区域就如同一个独立的网络，该区域的 OSPF 路由器只保存该区域的链路状态。每个路由器的链路状态数据库都可以保持合理的大小，路由计算的时间、报文数量都不会过大。

OSPF 网络类型：根据路由器所连接的物理网络不同，OSPF 将网络划分为四种类型：广播多路访问型（Broadcast Multi-Access，BMA）、非广播多路访问型（None Broadcast Multi-Access，NBMA）、点到点型（Point-to-Point）、点到多点型（Point-to-Multi-Point）。

广播多路访问型网络有 Ethernet、Token Ring、FDDI 等。NBMA 型网络有 Frame Relay、X. 25、SMDS 等。Point-to-Point 型网络有 PPP、HDLC 等。

指派路由器（Designated Router，DR）和备份指派路由器（Backup Designated Router，BDR）：在多路访问网络上可能存在多个路由器，为了避免路由器之间建立完全相邻关系而引起的大量开销，OSPF 要求在区域中选举一个 DR。每个路由器都与之建立完全相邻关系。DR 负责收集所有的链路状态信息，并发布给其他路由器。选举 DR 的同时也选举出一个 BDR，在 DR 失效的时候，BDR 担负起 DR 的职责。点对点型网络不需要 DR，因为只存在两个节点，彼此间完全相邻。协议组由 OSPF 协议、Hello 协议、交换协议、扩散协议组成。

现以 Hello 协议为例，具体介绍一下。当路由器开启一个端口的 OSPF 路由时，将会从这个端口发出一个 Hello 报文，以后它也将以一定的间隔周期性地发送 Hello 报文。OSPF 路由器用 Hello 报文来初始化新的相邻关系以及确认相邻的路由器邻居之间的通信状态。

对广播多路访问型网络和非广播多路访问型网络，路由器使用 Hello 协议选举出一个 DR。在广播型网络里，Hello 报文使用多播地址 224.0.0.5 周期性广播，并通过这个过程自动发现路由器邻居。在 NBMA 网络中，DR 负责向其他路由器逐一发送 Hello 报文。

OSPF 路由协议一般用于同一个自治域(AS)内，在这个 AS 中，所有的路由器都维护一个相同的描述这个 AS 结构的数据库，该数据库中存放的是路由域中相应链路的状态信息，称为链路状态数据库。路由器通过这个数据库计算出其 OSPF 路由表。

一种链路状态的路由协议，OSPF 将链路状态广播数据包(Link-State Advertisement，LSA)传送给在某一区域内的所有路由器，这一点与距离矢量路由协议不同，距离矢量路由协议的路由器是将部分或全部的路由表传递给与其相邻的路由器。

OSPF 路由协议的数据包格式如表 6-1 所示。

**表 6-1　OSPF 路由协议数据包格式**

| Version Num | Type | Packet Length | Router ID | AreaID | Check Sum | Authentication Type | Authentication |
|---|---|---|---|---|---|---|---|

Version Num——定义所采用的 OSPF 路由协议的版本。

Type ——定义 OSPF 数据包类型。OSPF 数据包共有 5 种：

(1) Hello——用于建立和维护相邻的两个 OSPF 路由器的关系，该数据包是周期性地发送的。

(2) Database Description ——用于描述整个数据库，该数据包仅在 OSPF 初始化时发送。

(3) Link State Request ——用于向相邻的 OSPF 路由器请求部分或全部的数据，这种数据包是在当路由器发现其数据已经过期时才发送的。

(4) Link State Update——这是对 Link State 请求数据包的响应，即通常所说的 LSA 数据包。

(5) Link State Acknowledgment——是对 LSA 数据包的响应。

Packet Length——定义整个数据包的长度。

Router ID——用于描述数据包的源地址，以 IP 地址来表示。

Area ID——用于区分 OSPF 数据包属于的区域号，所有的 OSPF 数据包都属于一个特定的 OSPF 区域。

Check Sum——校验和，用于标记数据包在传递时有无误码。

Authentication Type——定义 OSPF 验证类型。

Authentication ——包含 OSPF 验证信息，长为 8 个字节。

SPF 算法：SPF 算法是 OSPF 路由协议的基础。SPF 算法有时也被称为 Dijkstra 算法，这是因为最短路径优先算法 SPF 是 Dijkstra 发明的。SPF 算法将每一个路由器作为根(Root)来计算其到每一个目的地路由器的距离，每一个路由器根据一个统一的数据库会计算出路由域的拓扑结构图，该结构图类似于一棵树，在 SPF 算法中，被称为最短路径树。

链路状态算法作为一种典型的链路状态的路由协议，OSPF 还得遵循链路状态路由协议的统一算法。链路状态的算法非常简单，在这里将链路状态算法概括为以下四个步骤。

(1) 当路由器初始化或当网络结构发生变化(例如增减路由器，链路状态发生变化等)时，路由器会产生链路状态广播数据包 LSA，该数据包里包含路由器上所有相连链路，即为所有端口的状态信息。

(2) 所有路由器会通过一种被称为刷新(Flooding)的方法来交换链路状态数据。Flooding 是指路由器将其 LSA 数据包传送给所有与其相邻的 OSPF 路由器，相邻路由器根据其接收到的链路状态信息更新自己的数据库，并将该链路状态信息转送给与其相邻的路由器，直至稳定的一个过程。

(3) 当网络重新稳定下来，也可以说 OSPF 路由协议收敛下来时，所有的路由器会根据其各自的链路状态信息数据库计算出各自的路由表。该路由表中包含路由器到每一个可到达目的地的 Cost 以及到达该目的地所要转发的下一个路由器。

(4) 当网络状态比较稳定时，网络中传递的链路状态信息是比较少的。这也正是链路状态路由协议区别于距离矢量路由协议的一大特点。

OSPF 配置语句：

```
R1(config)# router ospf process-id
```

Process id：是一个介于 1 和 65 535 之间的数字，由网络管理员选定。Process id 仅在本地有效，这意味着路由器之间建立相邻关系时无需匹配该值。

```
Router(config-router)# network network-address wildcard-mask area area-id
```

通配符掩码：网络地址和通配符掩码一起，用于指定此 network 命令启用的接口或接口范围。

area：OSPF 区域是共享链路状态信息的一组路由器。OSPF 网络也可配置为多区域。

area-id：如果所有路由器都处于同一个 OSPF 区域，则必须在所有路由器上使用相同的 area-id 来配置 network 命令，比较好的做法是在单区域 OSPF 中使用 area-id 0。

OSPF 数据包可以通过认证来防止有意或无意地引入有害路由信息影响。认证作用有两点：

(1) 增加网络安全性(推荐使用 MD5)。

(2) 对 OSPF 重新配置时，不同口令可以配置在新口令和旧口令的路由器上，防止它们在一个共享的公共广播网络的情况下互相通信。

OSPF 路由认证有三种：Null (也就是不认证)、明文认证、MD5 加密校验和。

认证的配置注意事项：如果在一个区域内某处配置了认证，必须在整个区域配置认证；在一个区域里，可以在不同网络链路使用不同口令，邻居路由器之间配置相同的口令。

# 实验5　CLI 的使用与 IOS 基本命令

## 1. 实验目标

通过本实验，读者可以掌握如下技能：

(1) 熟悉路由器 CLI 的各种模式。

(2) 熟悉路由器 CLI 各种编辑命令。

(3) 掌握路由器的 IOS 基本命令。

(4) 查看路由器的有关信息。

## 2. 实验拓扑

实验拓扑如图 6-5 所示。

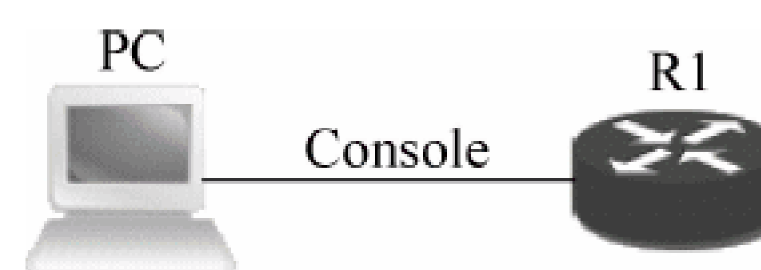



图 6-5　IOS 基本命令

## 3. 实验步骤

步骤 1：用户模式和特权模式的切换。

```
Router>
Router>enable
Router#
Router#disable
Router>
```

//"Router"是路由器的名字，而">"代表是在用户模式."enable"命令可以使路由器从用户模式进入到特权模式，"disable"命令则相反，在特权模式下的提示符为"#".

步骤 2："?"和 Tab 键的使用，以配置路由器时钟为例。

```
Router>enable
Router#clok
Translating "clok"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address.
```

//以上表明输入了错误的命令.

```
Router#cl?
clear clock
```

//路由器列出了当前模式下可以使用的以"cl"开头的所有命令.

```
Router#clock
% Incomplete command.
```

//路由器提示命令输入不完整.

```
Router#clock ?
set Set the time and date
```

//要注意的是"?"和"clock"之间要有空格，否则得到将不同的结果，如果不加空格路由器以为你是想列出以"clock"字母开头的命令，而不是想列出"clock"命令的子命令或参数.

```
Router#clock set ?
```

hh:mm:ss Current Time

Router# **clock set 11:36:00**

% Incomplete command.

Router# **clock set 11:36:00 ?**

<1-31> Day of the month

MONTH Month of the year

Router# **clock set 11:36:00 12 ?**

MONTH Month of the year

//以上多次使用"?"帮助命令，获得了"clock"命令的格式.

Router# **clock set 11:36:00 12 august**

% Incomplete command.

Router# **clock set 11:36:00 12 august 2011**

Router# **show clock**

11:36:03.149 UTC Tue Aug 12 2011

//到此成功配置了路由器的时钟，通常如果命令成功，路由器不会有任何提示. 在 CLI 下，可以直接使用"?"命令获得当前模式下的全部命令. 如下所示.

Router# ?

Exec commands:

access-enable Create a temporary Access-List entry

access-profile Apply user-profile to interface

access-template Create a temporary Access-List entry

……………………………………………//为了节约篇幅，此处省略了部分输出.

erase Erase a filesystem

exit Exit from the EXEC

help Description of the interactive help system

--More—

//有多于一屏的内容时，按"回车"键显示下一行，按"空格"显示下一页，其他键则退出.

Router# disable

Router>**en**

Router#

//在 CLI 中，命令是可以缩写的，但前提是路由器要能够区分得出，如下所示.

Router# **dis**

% Ambiguous command: "dis".

Router# **dis?**

disable disconnect

//使用 dis 不能退出特权模式的原因是路由器无法区分出 dis 代表 disable 还是 disconnect. 若再加多一个字母 a 就可以区分了.

Router# **disa**

Router>**en【Tab】**

Router>**enable**

Router# **conf【Tab】**

Router# **configure t【Tab】**

Router# **configure terminal**

Router(config)#

//可以使用 Tab 键帮助我们自动完成命令.

步骤 3：IOS 编辑命令与历史命令缓存大小。

```
Router# show history
en
conf t
show history
disable
enable
conf t
show history
//以上是显示历史命令.
```

# 实验 6　路由器的基本配置

**1. 实验目标**

通过本实验，应当掌握能够通过 Console 接口对路由器进行初始配置，能够熟练使用路由器的各种口令，能够对路由器进行基本配置，可以使用 show 命令查看路由器的状态。

**2. 实验拓扑**

实验拓扑如图 6-6 所示。



图 6-6　路由器的基本配置

**3. 实验的准备**

Cisco 1841 路由器（一台）

PC（一台）

交叉线（一根）

Console 线（一根）

**4. 实验过程**

1）设备连接

按照图 6-6 通过 Console 线把路由器的 Console 端口和 Com 端口连接，交叉线将 PC 的网口和路由器的 f0/0 接口连接。

2）设备加电

通过超级终端查看路由器启动过程。

```
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1,
RELEASE SOFTWARE (fc2)
```

```
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
         --- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]:
```

输入 NO,两次回车 将出现:

```
Press RETURN to get started!
Router>
```

将路由器的主机名改为 R1:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
```

3）配置路由器的各种口令

配置访问特权模式密码。

（1）使能口令

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
R1(config)#enable password cisco
```

（2）使能加密口令

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
R1(config)#enable secret cisco123
R1#show running-config
Building configuration...
Current configuration : 517 bytes!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R1
enable secret 5 $1$mERr$5.a6P4JqbNiMX01usIfka/
enable password cisco
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
```

```
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
line con 0
line vty 0 4
 login
end
```

(3) 配置控制台口令。

```
R1>enable
R1#configure terminal
R1(config)#line console 0
R1(config-line)#password cisco456
R1(config-line)#login
```

(4) 配置 telnet 口令。

```
R1>enable
R1#configure terminal
R1(config)#line vty 0 4
R1(config-line)#password cisco789
R1(config-line)#login
```

(5) 路由器接口地址配置。

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#no shutdown                    //接口缺省状态下是关闭的
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
R1(config-if)#ip address 172.16.1.1 255.255.255.0
```

PC 配置地址如图 6-7 所示。

(6) 通过 Telnet 方式验证各种密码。依次单击“开始”→“运行”,输入 cmd,单击“确定”按钮,进行命令行窗口,输入 telnet 172.16.1.1,如图 6-8 所示。

```
PC>telnet 172.16.1.1
Trying 172.16.1.1 ...Open
User Access Verification
```

图 6-7　PC 默认网关的配置




图 6-8　进入命令行窗口

Password:
输入 telnet 口令 cisco789.
Password:
R1>**enable**
Password:
输入使能加密口令 cisco123.
R1#
使用 show running-config 命令查看 R1 运行配置文件.
R1#**show running-config**

```
Building configuration...
Current configuration : 567 bytes
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R1
enable secret 5 $1$mERr$5.a6P4JqbNiMX01usIfka/
enable password cisco
interface FastEthernet0/0
 ip address 172.16.1.1 255.255.255.0
 duplex auto
 speed auto
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface Vlan1
 no ip address
 shutdown
ip classless
line con 0
 password cisco456
line vty 0 4
 password cisco789
 login
end
R1#
```

# 实验 7　静态路由配置

## 1. 实验目标

通过本实验，应当掌握静态路由协议的基本配置；可以使用 show ip route 命令查看路由表的状态；PC 之间可以互相通信。

**2. 实验拓扑**

实验拓扑如图 6-9 所示。

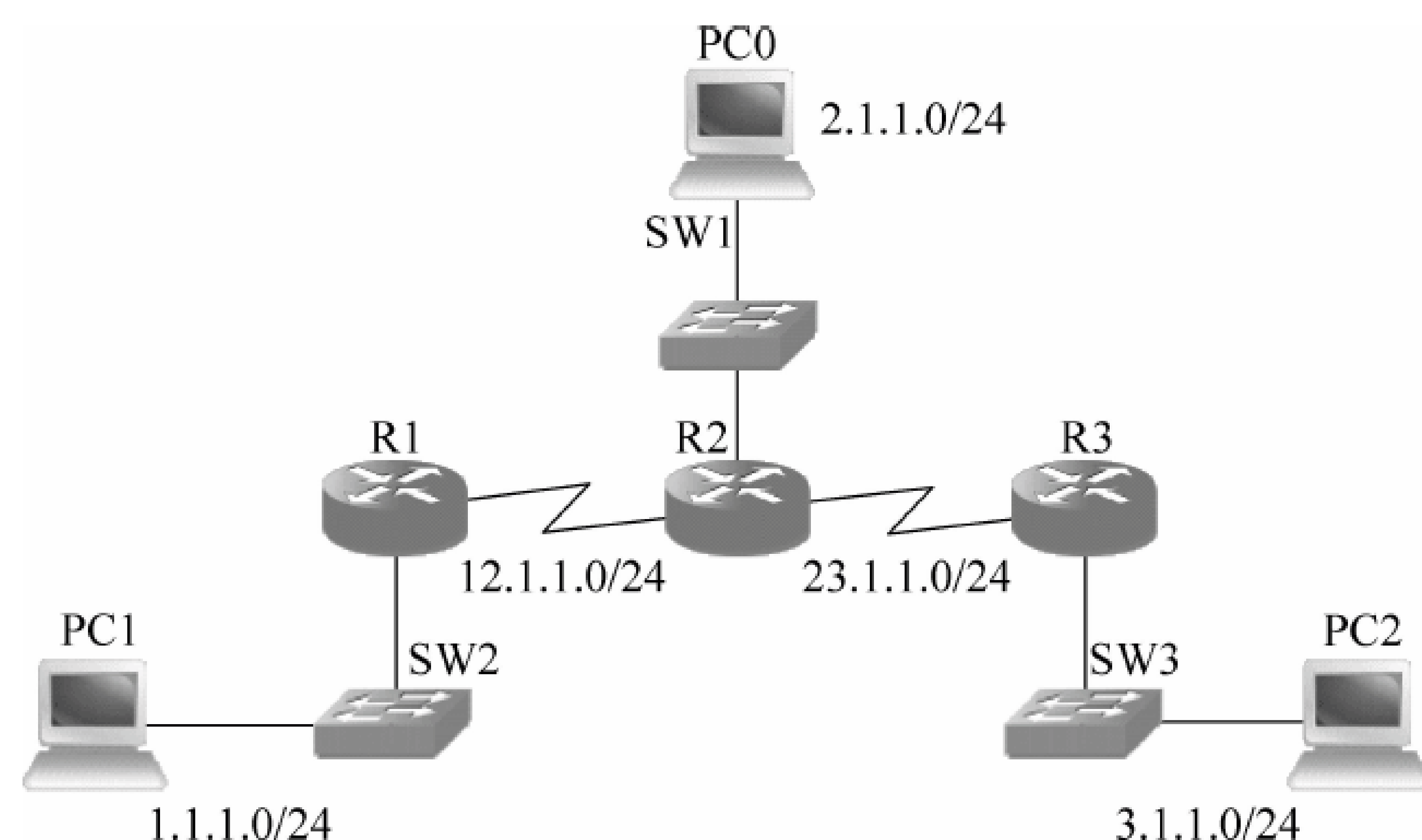



图 6-9 静态路由拓扑图

**3. 实验准备**

Cisco 1841 路由器(三台)

PC(三台)

串行线(两根)

直通线(三根)

**4. 实验过程**

**R1** :

Router>

Router>**enable**

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**hostname R1** //为路由器配置主机名

R1(config)#**interface f0/0**

R1(config-if)#**no shutdown** //建议在进到接口后立即开启接口

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

R1(config-if)#**ip address 1.1.1.1 255.255.255.0**

R1(config-if)#**exit**

R1(config)#**interface s0/0/0**

R1(config-if)#**no shutdown**

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

R1(config-if)#**ip address 12.1.1.1 255.255.255.0**

**R2**:

Router>

```
Router>en
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#interface s0/0/0
R2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
R2(config-if)#ip address 12.1.1.2 255.255.255.0
R2(config-if)#clock rate 64000            //配置时钟频率,模拟 DCE
R2(config-if)#exit
R2(config)#interface f0/0
R2(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R2(config-if)#ip address 2.1.1.1 255.255.255.0
R2(config-if)#exit
R2(config)#interface s0/0/1
R2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R2(config-if)#ip address 23.1.1.2 255.255.255.0
```

**R3:**

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#interface s0/0/1
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
Router(config-if)#ip address 23.1.1.3 255.255.255.0
Router(config-if)#clock rate 64000
Router(config-if)#exit
Router(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up in
Router(config)#interface f0/0
Router(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#ip address 3.1.1.1 255.255.255.0
Router(config-if)#exit
Router(config)#hostname R3
R3(config)#end
```

PC0 地址配置：

2.1.1.11　IP 地址
255.255.255.0　子网掩码
2.1.1.1　　网关

PC1 地址配置：

1.1.1.11　IP 地址
255.255.255.0　子网掩码
1.1.1.1　网关

PC2 地址配置：

3.1.1.11　IP 地址
255.255.255.0　子网掩码
3.1.1.1　　网关

配置静态路由：

R1：
R1(config) # **ip route 2.1.1.0 255.255.255.0 12.1.1.2**
R1(config) # **ip route 23.1.1.0 255.255.255.0 12.1.1.2**
R1(config) # **ip route 3.1.1.0 255.255.255.0 12.1.1.2**

R2：
R2(config) # **ip route 1.1.1.0 255.255.255.0 12.1.1.1**
R2(config) # **ip route 3.1.1.0 255.255.255.0 23.1.1.3**

R3：
R3(config) # **ip route 12.1.1.0 255.255.255.0 23.1.1.2**
R3(config) # **ip route 1.1.1.0 255.255.255.0 23.1.1.2**
R3(config) # **ip route 2.1.1.0 255.255.255.0 23.1.1.2**

R1 路由表：

```
R1 # show ip route                              //查看路由表
     1.0.0.0/24 is subnetted, 1 subnets
C        1.1.1.0 is directly connected, FastEthernet0/0
     2.0.0.0/24 is subnetted, 1 subnets
S        2.1.1.0 [1/0] via 12.1.1.2
     3.0.0.0/24 is subnetted, 1 subnets
S        3.1.1.0 [1/0] via 12.1.1.2
     12.0.0.0/24 is subnetted, 1 subnets
C        12.1.1.0 is directly connected, Serial0/0/0
     23.0.0.0/24 is subnetted, 1 subnets
```

```
S        23.1.1.0 [1/0] via 12.1.1.2
```

R2 路由表：

```
R2#show ip route
     1.0.0.0/24 is subnetted, 1 subnets
S        1.1.1.0 [1/0] via 12.1.1.1
     2.0.0.0/24 is subnetted, 1 subnets
C        2.1.1.0 is directly connected, FastEthernet0/0
     3.0.0.0/24 is subnetted, 1 subnets
S        3.1.1.0 [1/0] via 23.1.1.3
     12.0.0.0/24 is subnetted, 1 subnets
C        12.1.1.0 is directly connected, Serial0/0/0
     23.0.0.0/24 is subnetted, 1 subnets
C        23.1.1.0 is directly connected, Serial0/0/1
```

R3 路由表：

```
R3#show ip route
     1.0.0.0/24 is subnetted, 1 subnets
S        1.1.1.0 [1/0] via 23.1.1.2
     2.0.0.0/24 is subnetted, 1 subnets
S        2.1.1.0 [1/0] via 23.1.1.2
     3.0.0.0/24 is subnetted, 1 subnets
C        3.1.1.0 is directly connected, FastEthernet0/0
     12.0.0.0/24 is subnetted, 1 subnets
S        12.1.1.0 [1/0] via 23.1.1.2
     23.0.0.0/24 is subnetted, 1 subnets
C        23.1.1.0 is directly connected, Serial0/0/1
```

PC 之间可以互相通信，实验结束。

配置默认静态路由：

```
R1:
删除静态路由:
R1(config)# no ip route 2.1.1.0 255.255.255.0 12.1.1.2
R1(config)#no ip route 23.1.1.0 255.255.255.0 12.1.1.2
R1(config)#no ip route 3.1.1.0 255.255.255.0 12.1.1.2
添加默认静态路由:
R1(config)#ip route 0.0.0.0 0.0.0.0 12.1.1.2
```

查看 R1 路由表：

```
R1#show ip route
     1.0.0.0/24 is subnetted, 1 subnets
C        1.1.1.0 is directly connected, FastEthernet0/0
```

```
     12.0.0.0/24 is subnetted, 1 subnets
C         12.1.1.0 is directly connected, Serial0/0/0
S    0.0.0.0/0 [1/0] via 12.1.1.2
```

主机之间仍然能够正常通信,实验结束。

默认静态路由可以减小路由表的条目,常用在网络的出口。

# 实验 8　RIPv1 基本配置

**1. 实验目标**

通过本实验可以掌握:

(1) RIPv1 的配置。

(2) 理解路由表的含义。

(3) 查看和调试 RIPv1 路由协议相关信息。

(4) 掌握被动接口的配置方法。

(5) 理解被动接口的作用。

**2. 拓扑结构**

拓扑结构如图 6-10 所示。

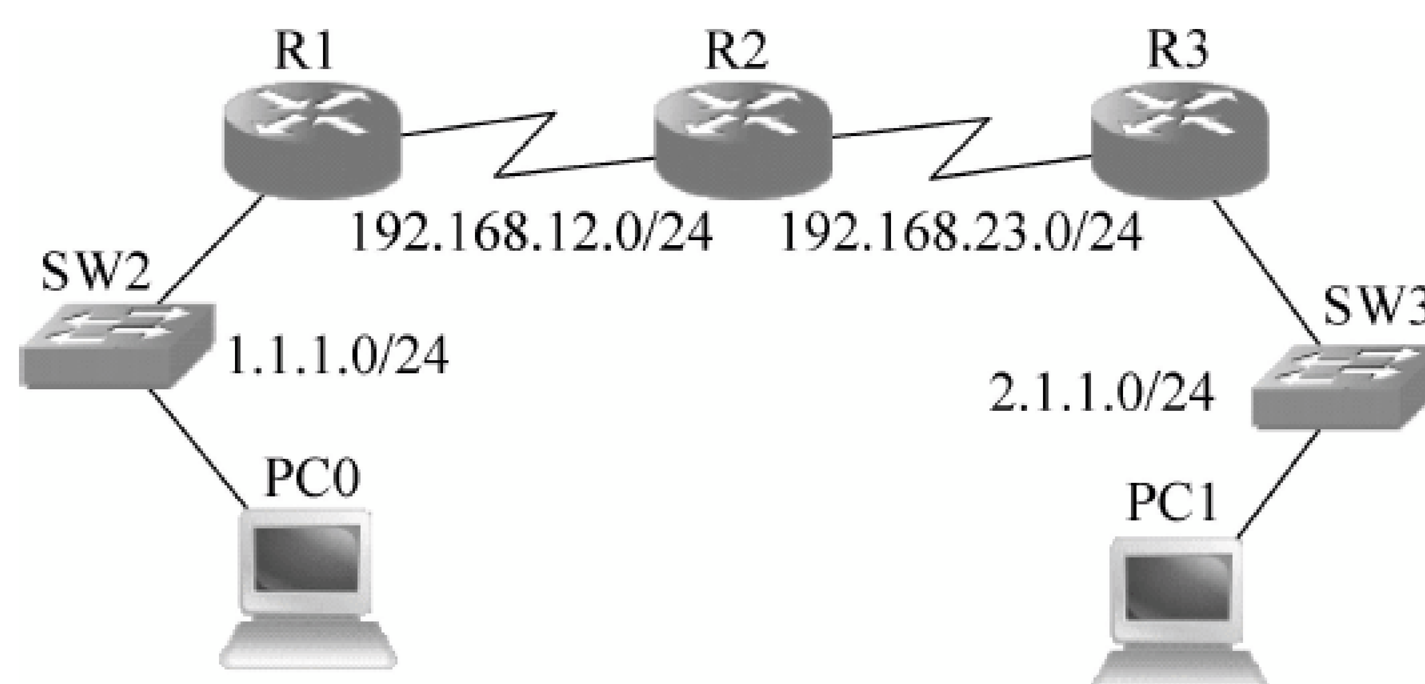



图 6-10　RIPv1 拓扑图

**3. 实验准备**

Cisco 1841 路由器(三台)

交换机(两台)

PC(两台)

串行线(两根)

直通线(四根)

**4. 试验步骤**

R1:

R1(config)# **router rip**　　　　　　　　　　//启动 RIP 进程

```
R1(config-router)#network 1.0.0.0           //宣告直连网段
R1(config-router)#network 192.168.12.0

R2:
R2(config)#router rip
R2(config-router)#network 192.168.12.0
R2(config-router)#network 192.168.23.0

R3:
R3(config)#router rip
R3(config-router)#network 192.168.23.0
R3(config-router)#network 2.0.0.0
```

查看 R1 路由表：

```
R1#show ip route
Gateway of last resort is not set
1.0.0.0/24 is subnetted, 1 subnets
C       1.1.1.0 is directly connected, FastEthernet0/0
R    2.0.0.0/8 [120/2] via 192.168.12.2, 00:00:07, Serial0/0/0
C    192.168.12.0/24 is directly connected, Serial0/0/0
R    192.168.23.0/24 [120/1] via 192.168.12.2, 00:00:07, Serial0/0/0
R    2.0.0.0/8 [120/2] via 192.168.12.2, 00:00:07, Serial0/0/0
```

R：通过 RIP 协议学习到的。

2.0.0.0/8：目的网络号。

120：RIP 的默认管理距离。

2：度量值，RIP 的度量是基于跳数，2 表示经过了 2 跳。

via 192.168.12.2：下一跳地址为 192.168.12.2。

00:00:07：更新时间，RIP 更新时间为 30s，23s 后再次更新。

Serial0/0/0：本路由器的出接口。

查看 R2 路由表：

```
R2#show ip route
Gateway of last resort is not set
R    1.0.0.0/8 [120/1] via 192.168.12.1, 00:00:14, Serial0/0/0
R    2.0.0.0/8 [120/1] via 192.168.23.3, 00:00:19, Serial0/0/1
C    192.168.12.0/24 is directly connected, Serial0/0/0
C    192.168.23.0/24 is directly connected, Serial0/0/1
```

查看 R3 路由表：

```
R3#show ip route
Gateway of last resort is not set
R    1.0.0.0/8 [120/2] via 192.168.23.2, 00:00:11, Serial0/0/1
```

```
     2.0.0.0/24 is subnetted, 1 subnets
C        2.1.1.0 is directly connected, FastEthernet0/0
R     192.168.12.0/24 [120/1] via 192.168.23.2, 00:00:11, Serial0/0/1
C     192.168.23.0/24 is directly connected, Serial0/0/1
```

由于 R1 和 R3 的以太网接口连接主机，不需要向这些接口发送路由更新，主机也读不懂路由更新，并且浪费带宽。所以，可以考虑将 R1 和 R3 的以太网接口设置为被动接口。

先把 R1 的 f0/0 接口配置为被动接口：

```
R1(config-router)#passive-interface fastEthernet 0/0
```

实验调试：

```
R1#debug ip rip
R1#clear ip route *
RIP: sending  v1 update to 255.255.255.255 via Serial0/0/0 (192.168.12.1)
RIP: build update entries
network 1.0.0.0 metric 1
RIP: received v1 update from 192.168.12.2 on Serial0/0/0
   2.0.0.0 in 2 hops
192.168.23.0 in 1 hops
```

可以看到 R1 确实不向被动接口 f0/0 发送路由更新。

```
R3#debug ip rip
RIP protocol debugging is on
R3#clear ip route *
R3#RIP: sending  v1 update to 255.255.255.255 via Serial0/0/1 (192.168.23.3)
RIP: build update entries
network 2.0.0.0 metric 1
RIP: sending  v1 update to 255.255.255.255 via FastEthernet0/0 (2.1.1.1)
RIP: build update entries
network 192.168.23.0 metric 1
RIP: received v1 update from 192.168.23.2 on Serial0/0/1
        1.0.0.0 in 2 hops
        192.168.12.0 in 1 hops
R3#undebug all                    //关闭 debug
```

没有做被动接口的 R3 仍然会向 F0/0 接口发送路由更新。

PC 之间可以互相通信实验结束。

## 实验 9　RIPv2 基本配置

### 1. 实验目标

通过本实验可以掌握：

（1）在路由器上启动 RIPv2 路由进程。
（2）启用参与路由协议的接口，并且通告网络。
（3）Auto-Summary 的开启和关闭。
（4）查看和调试 RIPv2 路由协议相关信息。

**2. 实验拓扑**

实验拓扑如图 6-11 所示。

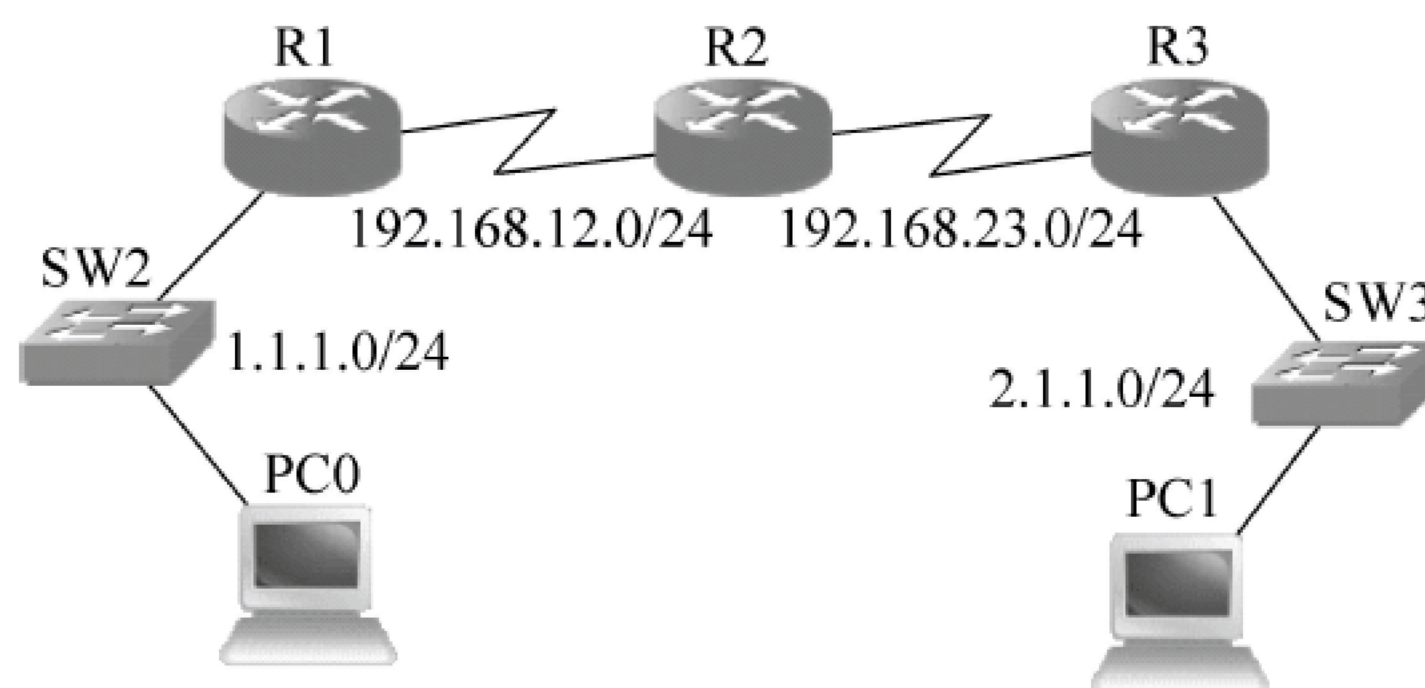



图 6-11　RIPv2 实验网络拓扑图

**3. 实验准备**

Cisco 1841 路由器（三台）
交换机（两台）
PC（两台）
串行线（两根）
直通线（四根）

**4. 实验步骤**

**R1：**
```
R1(config)# router rip                          //启动 RIP 进程
R1(config-router)# version 2                    //定义 RIP 版本 2
R1(config-router)# no auto-summary              //关闭自动汇总
R1(config-router)# network 1.0.0.0              //宣告直连网段
R1(config-router)# network 192.168.12.0
```

**R2：**
```
R2(config)# router rip
R2(config-router)# version 2
R2(config-router)# no auto-summary
R2(config-router)# network 192.168.12.0
R2(config-router)# network 192.168.23.0
```

**R3：**
```
R3(config)# router rip
R3(config-router)# version 2
```

```
R3(config-router)# no auto-summary
R3(config-router)# network 192.168.23.0
R3(config-router)# network 2.0.0.0
```

查看 R1 路由表:

```
R1# show ip route
Gateway of last resort is not set
     1.0.0.0/24 is subnetted, 1 subnets
C        1.1.1.0 is directly connected, FastEthernet0/0
R     2.0.0.0/8 [120/2] via 192.168.12.2, 00:00:07, Serial0/0/0
C     192.168.12.0/24 is directly connected, Serial0/0/0
R     192.168.23.0/24 [120/1] via 192.168.12.2, 00:00:07, Serial0/0/0
```

# 实验 10　RIPv2 汇总实验

**1. 实验目的**

通过本实验可以掌握:

(1) RIPv2 路由的手工汇总。

(2) 理解汇总的目的。

**2. 实验拓扑**

实验拓扑如图 6-12 所示。

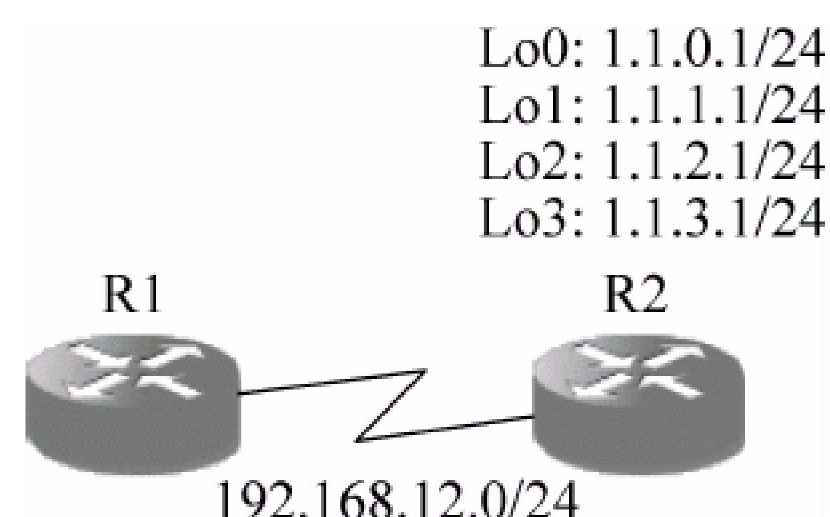



图 6-12　RIPv2 汇总实验拓扑

**3. 实验的准备**

Cisco 1841 路由器(两台)

串行线(一根)

**4. 设备调试**

设备基础配置略。

没做汇总之前查看 R1 路由表。

```
R1# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
     1.0.0.0/24 is subnetted, 4 subnets
R        1.1.0.0 [120/1] via 192.168.12.2, 00:00:21, Serial0/0/0
R        1.1.1.0 [120/1] via 192.168.12.2, 00:00:21, Serial0/0/0
```

```
R        1.1.2.0 [120/1] via 192.168.12.2, 00:00:21, Serial0/0/0
R        1.1.3.0 [120/1] via 192.168.12.2, 00:00:21, Serial0/0/0
C     192.168.12.0/24 is directly connected, Serial0/0/0
```

在 R2 上执行手动汇总。

```
R2(config-if)#ip summary-address rip 1.1.0.0 255.255.252.0
```

执行手动汇总后 R1 路由表。

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
     1.0.0.0/24 is subnetted, 4 subnets
R        1.1.0.0 [120/1] via 192.168.12.2, 00:00:21, Serial0/0/0
C     192.168.12.0/24 is directly connected, Serial0/0/0
```

R1 手动汇总路由实验结束。

# 实验 11　浮动静态路由

**1. 实验目标**

(1) 理解浮动静态路由原理。

(2) 熟悉浮动静态路由配置。

**2. 实验拓扑**

实验拓扑如图 6-13 所示。

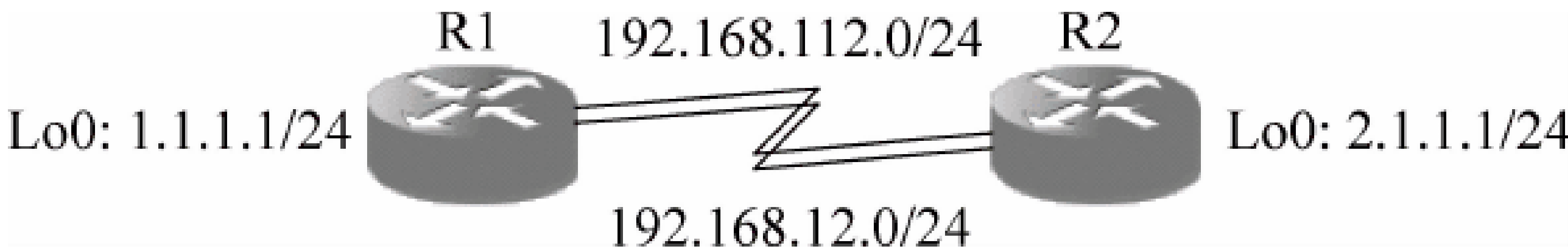



图 6-13　浮动静态路由实验拓扑

**3. 实验准备**

Cisco 1841 路由器(两台)

串行线(两根)

**4. 实验步骤**

将静态路由的管理距离设为 150,使得路由转发的时候走 RIP 协议,静态路由做备份。

```
R1:
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# no auto-summary
R1(config-router)# network 1.0.0.0
R1(config-router)# network 192.168.12.0
R1(config-router)# exit
R1(config)# ip route 2.1.1.0 255.255.255.0 192.168.112.2 150
//将静态路由的管理距离设为150

R2:
R2(config)# router rip
R2 (config-router)# version 2
R2 (config-router)# no auto-summary
R2 (config-router)# network 2.0.0.0
R2 (config-router)# network 192.168.12.0
R2 (config-router)# exit
R2r(config)# ip route 1.1.1.0 255.255.255.0 192.168.12.1 150
```

查看 R1 路由表:

```
R1# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set

1.0.0.0/24 is subnetted, 1 subnets
C        1.1.1.0 is directly connected, Loopback0
2.0.0.0/24 is subnetted, 1 subnets
R        2.1.1.0 [120/1] via 192.168.12.2, 00:00:01, Serial0/0/0
C     192.168.12.0/24 is directly connected, Serial0/0/0
C     192.168.112.0/24 is directly connected, Serial0/0/1
```

并没有看到静态路由,因为静态路由的管理比 RIP 大,所以静态路由处于隐藏备份状态。

将 R1 的 s0/0/0 接口关闭:

```
R1(config)# interface s0/0/0
```

```
R1(config-if)#sh
R1(config-if)#shutdown
```

查看 R1 路由表：

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
1.0.0.0/24 is subnetted, 1 subnets
C        1.1.1.0 is directly connected, Loopback0
2.0.0.0/24 is subnetted, 1 subnets
S        2.1.1.0 [150/0] via 192.168.112.2
C     192.168.112.0/24 is directly connected, Serial0/0/1
```

当主路由失效后，静态路由出现在路由表中，这说明了浮动静态路由的工作原理。

回复 R1 的 s0/0/0：

```
R1(config)#interface s0/0/0
R1(config-if)#no shutdown
```

查看 R1 路由表：

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
     1.0.0.0/24 is subnetted, 1 subnets
C        1.1.1.0 is directly connected, Loopback0
     2.0.0.0/24 is subnetted, 1 subnets
R        2.1.1.0 [120/1] via 192.168.12.2, 00:00:12, Serial0/0/0
C     192.168.12.0/24 is directly connected, Serial0/0/0
C     192.168.112.0/24 is directly connected, Serial0/0/1
```

RIP 路由回到路由表中，静态路由再次隐藏，实验结束。

# 实验 12　OSPF 基本配置

## 1. 实验目标

通过本实验可以掌握：

(1) 在路由器上启动 OSPF 路由进程。

(2) 启用参与路由协议的接口，并且通告网络及所在的区域。

(3) 度量值 Cost 的计算。

(4) Hello 相关参数的配置。

(5) 点到点链路上的 OSPF 的特征。

(6) 查看和调试 OSPF 路由协议相关信息。

## 2. 实验拓扑

实验拓扑如图 6-14 所示。

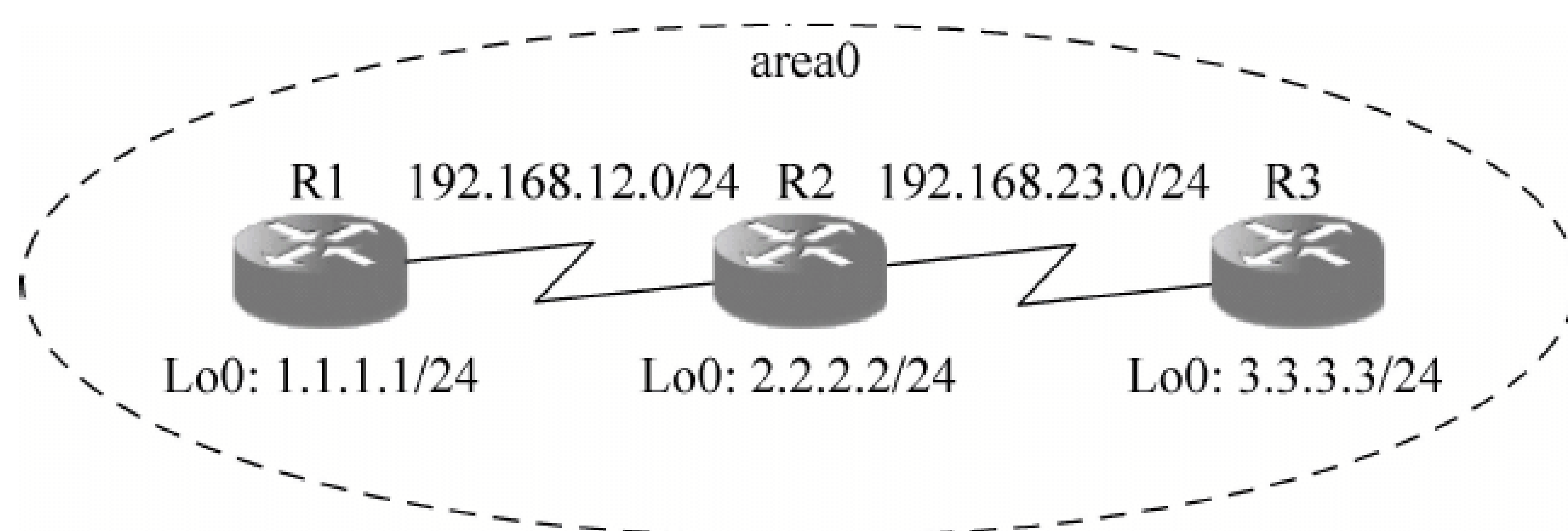



图 6-14　OSPF 基本配置实验拓扑图

## 3. 实验的准备

Cisco 1841 路由器(三台)

串行线(两根)

## 4. 实验步骤

```
R1:
R1(config)#router ospf 1                                  //进入 OSPF 进程
R1(config-router)#router-id 1.1.1.1                       //指定 RID
R1(config-router)#network 1.1.1.0 0.0.0.255 area 0        //宣告网络
R1(config-router)#network 192.168.12.0 0.0.0.255 area 0

R2:
R2(config)#router ospf 1
R2 (config-router)#router-id 2.2.2.2
R2 (config-router)#network 2.2.2.0 0.0.0.255 area 0
R2 (config-router)#network 192.168.12.0 0.0.0.255 area 0
R2 (config-router)#network 192.168.23.0 0.0.0.255 area 0
```

```
R3:
R3(config)# router ospf 1
R3(config-router)# router-id 3.3.3.3
R3(config-router)# network 192.168.23.0 0.0.0.255 area 0
R3(config-router)# network 3.3.3.0 0.0.0.255 area 0
R3(config)# router ospf 1
```

1 代表进程 ID,范围是 1-65 535,本地有意义。

```
R3(config-router)# router-id 3.3.3.3
```

router-id：路由器的 ID,选举过程是如果在路由进程中指定,就使用指定地址,如果没指定就选环回接口地址最大的,如果也没有环回接口,那么选择物理接口最大的地址作为 RID,建议直接在路由进程中指定,这样可控性较好。

```
R3(config-router)# network 3.3.3.0 0.0.0.255 area 0
```

area 0：区域 ID 是在 0-4 294 967 295,area 0 代表骨干区域。

设备调试：

查看 R1 路由表：

```
R1# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
     1.0.0.0/24 is subnetted, 1 subnets
C       1.1.1.0 is directly connected, Loopback0
     2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2 [110/65] via 192.168.12.2, 00:11:23, Serial0/0/0
     3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/129] via 192.168.12.2, 00:09:16, Serial0/0/0
C    192.168.12.0/24 is directly connected, Serial0/0/0
192.168.23.0/24 [110/128] via 192.168.12.2, 00:11:23, Serial0/0/0
```

可以看到学来了三条用“O”表示的路由,R2 学习到两条路由,R3 学习了三条路由。

查看 R2 邻居表：

```
R2# show ip ospf neighbor
Neighbor ID     Pri   State        Dead Time   Address         Interface
3.3.3.3         0     FULL/  -     00:00:31    192.168.23.3    Serial0/0/1
1.1.1.1         0     FULL/  -     00:00:34    192.168.12.1    Serial0/0/0
```

R2 有两个邻居，分别是 3.3.3.3 和 1.1.1.1，见到状态为 FULL 表示邻居关系建立成功。

实验结束。

# 实验 13　OSPF 简单口令认证

## 1. 实验目的

通过本实验可以掌握：

(1) OSPF 认证的类型和意义。

(2) 基于区域的 OSPF 简单口令认证的配置和调试。

## 2. 实验拓扑

实验拓扑如图 6-15 所示。

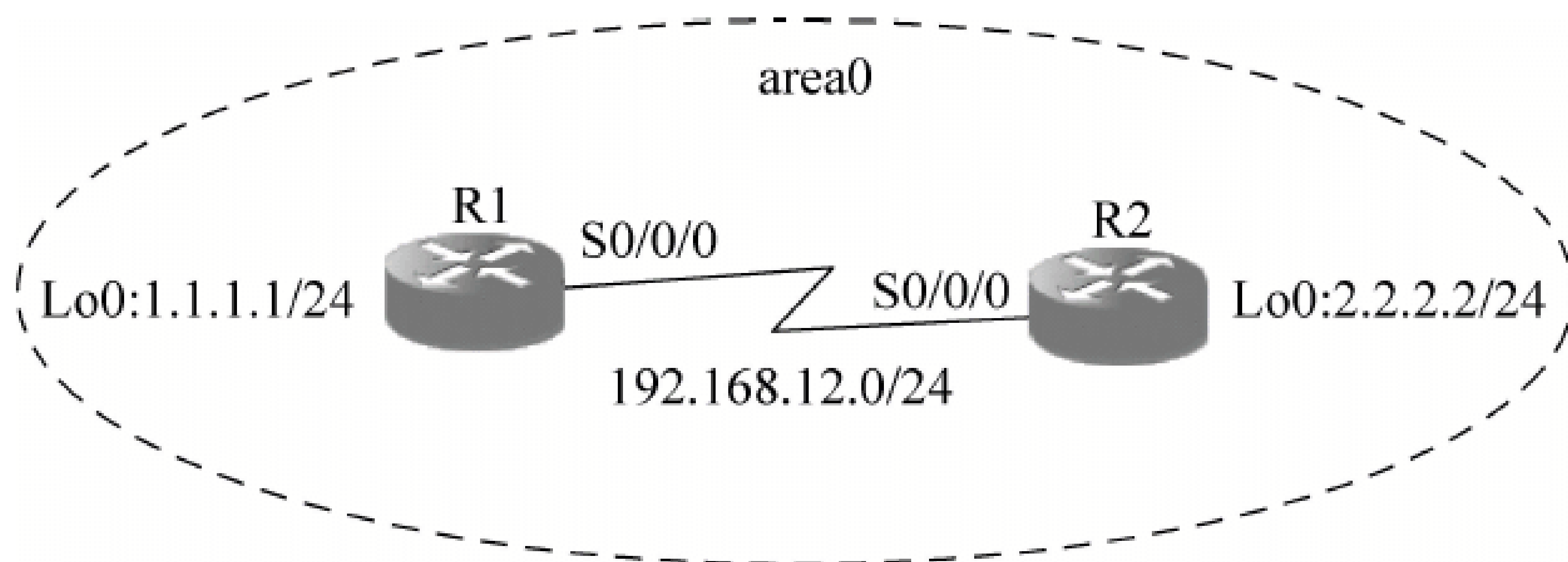



图 6-15　OSPF 简单口令认证实验拓扑图

## 3. 实验的准备

Cisco 1841 路由器(两台)

串行线(一根)

## 4. 实验步骤

```
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 192.168.12.0 255.255.255.0 area 0
R1(config-router)#network 1.1.1.0 255.255.255.0 area 0
R1(config-router)#area 0 authentication          //区域 0 启用简单口令认证
R1(config)#interface s0/0/0
R1(config-if)#ip ospf authentication-key cisco    //配置密码，密码为 Cisco

R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 2.2.2.0 255.255.255.0 area 0
R2(config-router)#network 192.168.12.0 255.255.255.0 area 0
R2(config-router)#area 0 authentication
R2(config)#interface s0/0/0
```

```
R2(config-if)# ip ospf authentication-key cisco
```

配置结束，如果两端口令不一致将不能建立邻居关系。

# 思考与练习

**一、填空题**

1. 集线器工作在 OSI 七层参考模型中的第________层。
2. 网桥工作在 OSI 七层参考模型中的________层。
3. 根据传输介质的不同，网卡出现了________接口、________接口和________接口三种接口类型。
4. 交换机通过直通式、________、碎片隔离三种方式进行转发数据。
5. 路由器工作在 OSI 七层参考模型中的________层。
6. 网络适配器又称________。
7. 路由器的硬件组成包括了________、内存、只读内存、闪存、________、________。

**二、选择题**

1. 以下哪项不是网卡的基本功能？(　　)
   A. 从并行到串行的数据转换
   B. 包的装配和拆装
   C. 数据缓存和网络信号
   D. 路由寻址
2. 根据网卡总线类型的不同，可以分为(　　)类。
   A. 2　　B. 3　　C. 4　　D. 5
3. 中继器工作在(　　)层。
   A. 物理　　B. 数据链路　　C. 网络　　D. 会话

**三、简答题**

1. 什么是网络互联？
2. 网络互联的形式有哪些？
3. 路由器加电启动过程？
4. 路由器的最基本功能是什么？完成该功能它需要做什么工作？
5. 影响动态路由选择的因素是什么？
6. 动态路由选择协议有哪几种，它们是如何进行通告更新和更新处理的？
7. 静态路由的优缺点有哪些？

第 7 章

# 传输层的主流协议

传输层负责网络传输，是应用层和网络层之间的桥梁。传输层为各应用层协议和服务提供端到端的连接支持。TCP/IP 协议簇中最常用的两种传输协议是传输控制协议（TCP）和用户数据报协议（UDP）。这两种协议都用于支持多个应用程序的通信，其不同点在于每个协议执行各自特定的功能。

## 7.1 传输层协议概述

TCP/IP 模型中，传输层位于应用层和网络层之间，传输层的 TCP 和 UDP 两大协议为各种应用层协议提供服务，如图 7-1 所示。传输层管理着网络主机之间端到端通信，负责将一端应用层产生的数据传递给对方应用层。

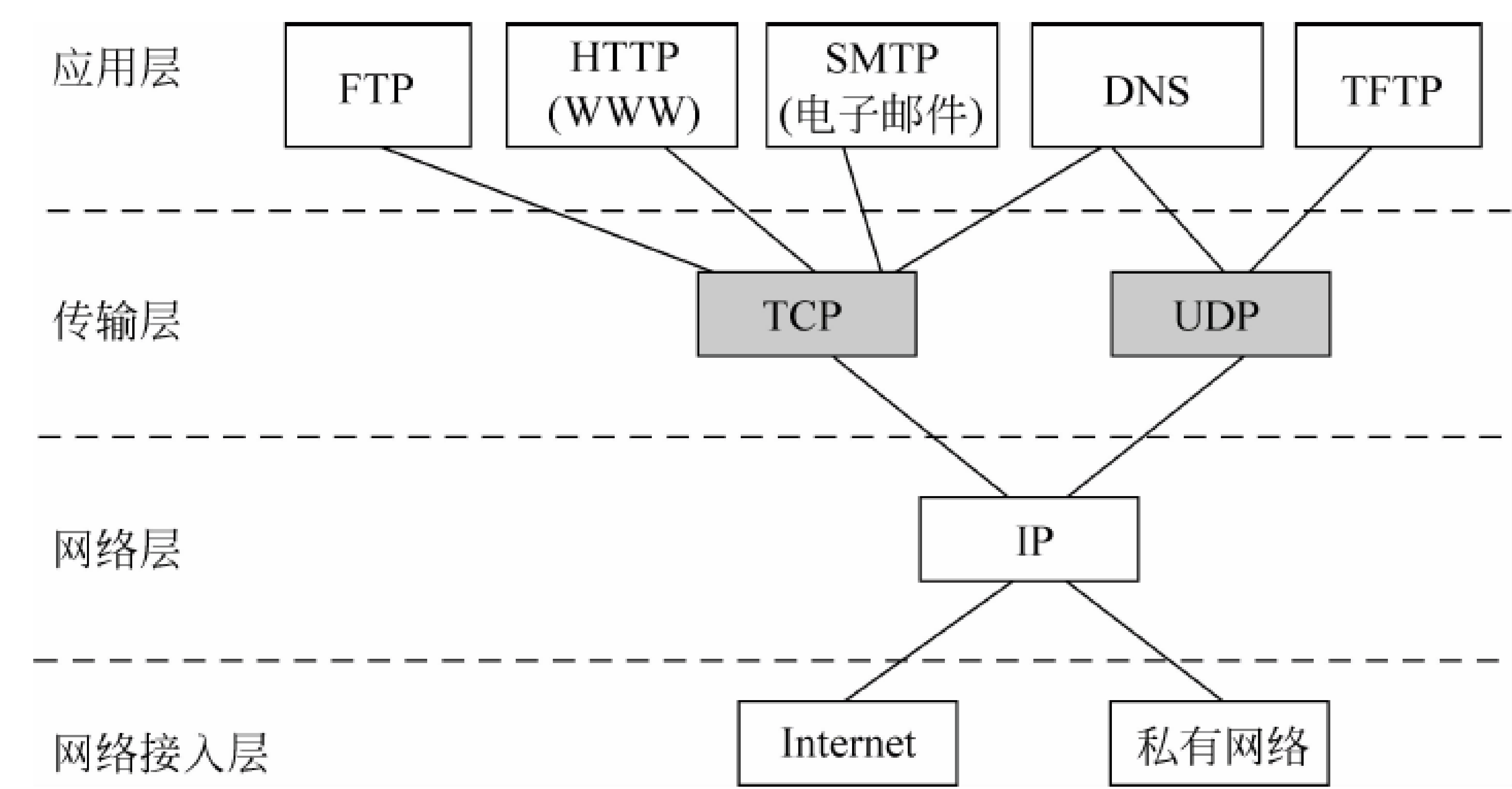



图 7-1 传输层在 TCP/IP 模型中的位置

### 7.1.1 传输层 PDU

传输层协议数据单元 PDU 是为了封装应用层数据的传输层数据传输单位，有 UDP 数据报和 TCP 数据段两种。两种 PDU 报头有很大差别。

**1. UDP 数据报**

UDP 数据报报头由 4 个字段组成，每个字段各占 2 字节。具体为：源端口号、目标端

口号、数据报长度、校验和，如图 7-2 所示。

<table>
<tr><td>源端口号(16)</td><td>目的端口号(16)</td></tr>
<tr><td>长度(16)</td><td>校验和(16)</td></tr>
<tr><td colspan="2">应用层数据(大小不等)</td></tr>
</table>

图 7-2　UDP 数据报格式

源端口号是本地主机上始发应用程序相关联的通信端口号；而目的端口号则是远程主机上目的应用程序相关联的通信端口号，UDP 协议使用端口号为不同的应用保留其各自的数据传输通道。

数据报的长度字段表示包括报头和数据部分在内的总的字节数，因为报头的长度是固定的(8 字节)，所以该字段主要被用来计算可变长度的应用层数据部分。

校验和字段用来保证数据的安全，校验值首先在数据发送方通过特殊的算法计算得出，在传递到接收方之后，还需要再重新计算，UDP 必须要有校验值。

**2. TCP 数据段**

TCP 报文段的报头有 10 个必需的字段和 1 个可选字段，报头至少为 20 字节，报头后面的数据是可选项。

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

<table>
<tr><td colspan="8">源端口号</td><td>目的端口号</td></tr>
<tr><td colspan="9">序列号</td></tr>
<tr><td colspan="9">确认号</td></tr>
<tr><td>数据<br>偏移值</td><td>保留</td><td>U<br>R<br>G</td><td>A<br>C<br>K</td><td>F<br>S<br>T</td><td>R<br>S<br>H</td><td>S<br>Y<br>N</td><td>F<br>I<br>N</td><td>窗口大小</td></tr>
<tr><td colspan="8">校验值</td><td>紧急数据指针</td></tr>
<tr><td colspan="9">选项＋填充</td></tr>
<tr><td colspan="9">应用层数据(大小不等)</td></tr>
</table>

图 7-3　TCP 数据段格式

1) 源端口号(16 位)

标识发送报文的计算机端口或进程，一个 TCP 报文段必须包括源端口号，源端口和源 IP 地址的作用是标识报文的返回地址，使目的主机知道应该向何处发送确认报文。

2) 目的端口号(16 位)

定义传输的目的，这个端口指明报文接收计算机上的应用程序端口或进程。

3) 序列号(32 位)

TCP 是面向字节流的，在一个 TCP 连接中传送的字节流中的每一个字节都按顺序编

号，序列号增加到 $2^{32}-1$ 后，下个序列号从 0 重新开始。整个要传送的字节流的起始序列号必须在连接建立的时候设置，序列号字段中的值指的是本报文段所发送数据的第一个字节的序列号。

4）确认号（32 位）

目的主机返回确认号，使源主机知道某个或几个报文段已被接收。如果 ACK 控制位被设置为 1，则该字段有效。确认号等于顺序接收到的最后一个报文段的序号加 1，这也是目的主机希望下次接收的报文段的序号值。返回确认号后，计算机认为已接收到小于该确认号的所有数据。例如：接收方收到一个报文段，其序列号是 401，数据长度是 100 字节（序列号为 401～500），表明接收方已接收到了发送方发送来的序列号为 500 为止的数据。因此，接收方希望接收到的下一个序列号是 501，而不是 500。

5）报文长度（4 位）

由于 TCP 报头的长度随 TCP 选项字段内容的不同而变化，因此报头中包含一个指定报头长度的字段。该字段以 32 比特为单位，所以报头长度一定是 32 比特的整数倍，有时需要在报头末尾补 0。如果报头没有 TCP 选项字段，则报头长度值为 5，表示报头一个有 160 比特，即 20 字节。

6）保留位（6 位）

这些位必须是 0，是为了将来定义新的用途所保留的。

7）控制位（6 位）

URG：紧急比特位。URG 为 1 时，表明紧急指针字段有效。它告诉系统此报文段中有紧急数据，应尽快传递。

ACK：确认比特位。ACK 为 1 时，表示确认号有效。

PSH：推送比特位。PSH 为 1 时，表示计算机要立即将数据交给应用进程，而不再等到整个缓存都填满后再向上推送。

RST：复位比特位。RST 为 1 时，表示 TCP 连接出现严重差错，必须释放连接，然后再重新建立连接。

SYN：同步比特位。SYN 为 1，表示这是一个连接请求或连接接受报文。此后的所有报文段中，SYN 都被置 0。

FIN：源主机不再有待发送的数据。如果源主机数据发送完毕，将把该连接下要发送的最后一个报文段的报头中的 FIN 位置 1，或将该报文段后面发送的报头中该位置 1。

8）窗口（16 位）

窗口指的是发送本报文段一方的接收窗口（不是自己的发送窗口），窗口值告诉对方从本报文段首部中的确认号算起，允许对方发送的数据量。窗口值作为让对方设置其发送窗口的依据，这个值也是经常动态变化的。

9）校验和（16 位）

源主机和目的主机根据 TCP 报文段以及伪报头的内容计算校验和。在伪报头中存放

着来自 IP 报头以及 TCP 报文段长度信息。与 UDP 一样,伪报头并不在网络中传输,并且在校验和中包含伪报头的目的是为了防止目的主机错误地接收存在错误的数据报。

10) 紧急指针(16 位)

如果 URG 为 1,则紧急指针标志着紧急数据的结束,其值是紧急数据最后 1 字节的序号,表示报文段序号的偏移量。例如,如果报文段的序号是 1000,前 8 个字节都是紧急数据,那么紧急指针就是 8。紧急指针一般用途是使用户可中止进程。

11) TCP 选项和填充(0 或更大)

TCP 选项长度不定,但长度必须以字节为单位存在;填充字段不定长,其内容必须为 0,完整的 TCP 报头必须是 32 比特的整数倍,为了达到这一要求,通常会填充若干位 0 以保证 TCP 报头是 32 位的整数倍。

12) 应用层数据部分

报头后面是可选的报文段数据部分,IP 协议标准可以接收最长达 576 字节的数据报。无其他选项的 IP 报头是 20 字节,无其他选项的 TCP 报头也是 20 字节,所以含有 536 字节以下数据的 TCP 报文段无须分片就可达到目的主机。

UDP 和 TCP 协议数据单元分别带有 8 字节和至少 20 字节的额外数据开销。正是由于具有不同的传输开销,这两种传输层协议提供不同效率、不同可靠性的传输服务:TCP 提供面向连接的可靠的、低效的传输;而 UDP 提供无连接的不可靠的、高效的传输服务。

### 7.1.2 传输层端口编址

端口号是一个 16 位的二进制数,其取值范围是 0～65 535。Internet 编号指派机构(The Internet Assigned Numbers Authority,IANA)负责分配端口号。其中 0～1023 是公认端口;1024～49 151 是已注册端口;49 152～65 535 是动态或私有端口。

**1. 公认端口**

公认端口(0～1023)也称知名端口,用于公共服务和应用程序。通过为服务器应用程序定义公认端口,可以将客户端应用程序设定为请求特定端口及其相关服务的连接。

表 7-1 列出了 TCP 和 UDP 的一些知名端口号及其对应的应用程序。

**表 7-1　知名端口**

| 知名端口 | 应 用 程 序 | 协议 |
|---|---|---|
| 20 | 文件传输协议(FTP)数据 | TCP |
| 21 | 文件传输协议(FTP)控制 | TCP |
| 23 | 远程登录协议(Telnet) | TCP |
| 25 | 简单邮件传输协议(SMTP) | TCP |
| 69 | 简单文件传输协议(TFTP) | UDP |
| 80 | 超文本传输协议(HTTP) | TCP |
| 110 | 邮局协议第 3 版(POP3) | TCP |

续表

| 知名端口 | 应 用 程 序 | 协议 |
|---|---|---|
| 194 | Internet 在线聊天(IRC) | TCP |
| 443 | 安全的 HTTP(HTTPS) | TCP |
| 520 | 路由信息协议(RIP) | UDP |

**2. 已注册端口**

已注册端口(1024～49 151)是分配给用户进程或应用程序的端口。这些进程主要是用户选择安装的一些应用程序,而不是已经分配了公认端口的常用应用程序。这些端口在没有被服务器占用时,可由客户端动态选用为源端口。

表 7-2 列出了 TCP 和 UDP 使用的已注册端口号。

**表 7-2 已注册端口**

| 注册端口 | 应 用 程 序 | 协议 |
|---|---|---|
| 1812 | RADIUS 身份验证 | UDP |
| 1863 | MSN Messenger | TCP |
| 2000 | 思科信令连接控制协议(SCCP,用在 VoIP 语音程序) | UDP |
| 5004 | 实时传输协议(RTP,语音与视频传输协议) | UDP |
| 5060 | 话路启动协议(SIP,用于 VoIP 应用程序) | UDP |
| 8008 | HTTP 备用 | TCP |
| 8080 | HTTP 备用 | TCP |

**3. 动态或私有端口**

动态或私有端口(49 152～65 535),也称临时端口。这些端口往往在开始连接时被动态分配给客户端应用程序作为源端口,客户端一般很少使用动态或私有端口连接服务器。

**4. 同时使用 TCP 和 UDP 的端口**

一些应用程序可能既使用 TCP,又使用 UDP。例如,通过低开销的 UDP,DNS 可以很快响应很多客户端的请求;但有时发送被请求的信息需要满足可靠性要求,此时该程序内的两种协议将同时采用公认端口号 53。

表 7-3 列出了常用的同时使用 TCP 和 UDP 的注册和知名端口号。

**表 7-3 同时使用 TCP 和 UDP 的端口**

| 常用端口 | 应 用 程 序 | 端 口 类 型 |
|---|---|---|
| 53 | DNS | 公认 TCP/UDP 常用端口 |
| 161 | 简单网络管理协议,SNMP | 公认 TCP/UDP 常用端口 |
| 531 | AOL 即时通信,IRC | 公认 TCP/UDP 常用端口 |
| 1433 | MS SQL | 已注册 TCP/UDP 常用端口 |
| 2948 | WAP(MMS) | 已注册 TCP/UDP 常用端口 |

# 7.2　传输控制协议 TCP

TCP 通常被称为面向连接的协议，这一协议保证可靠有序地将数据从发送者传送到接收者，TCP 通过创建可靠会话连接、窗口确认以及数据重传来实现可靠通信。

## 7.2.1　TCP 可靠连接

在 TCP/IP 协议中，TCP 协议提供可靠的面向连接的会话服务。在使用 TCP 会话之前，源主机和目的主机必须交换消息并建立连接，才能通过连接发送数据段，并在完成数据传输后拆除连接。

**1. 三次握手**

TCP 采用三次握手建立一个连接，一个完整的三次握手包括请求、应答确认、再次确认的过程，如图 7-4 所示。

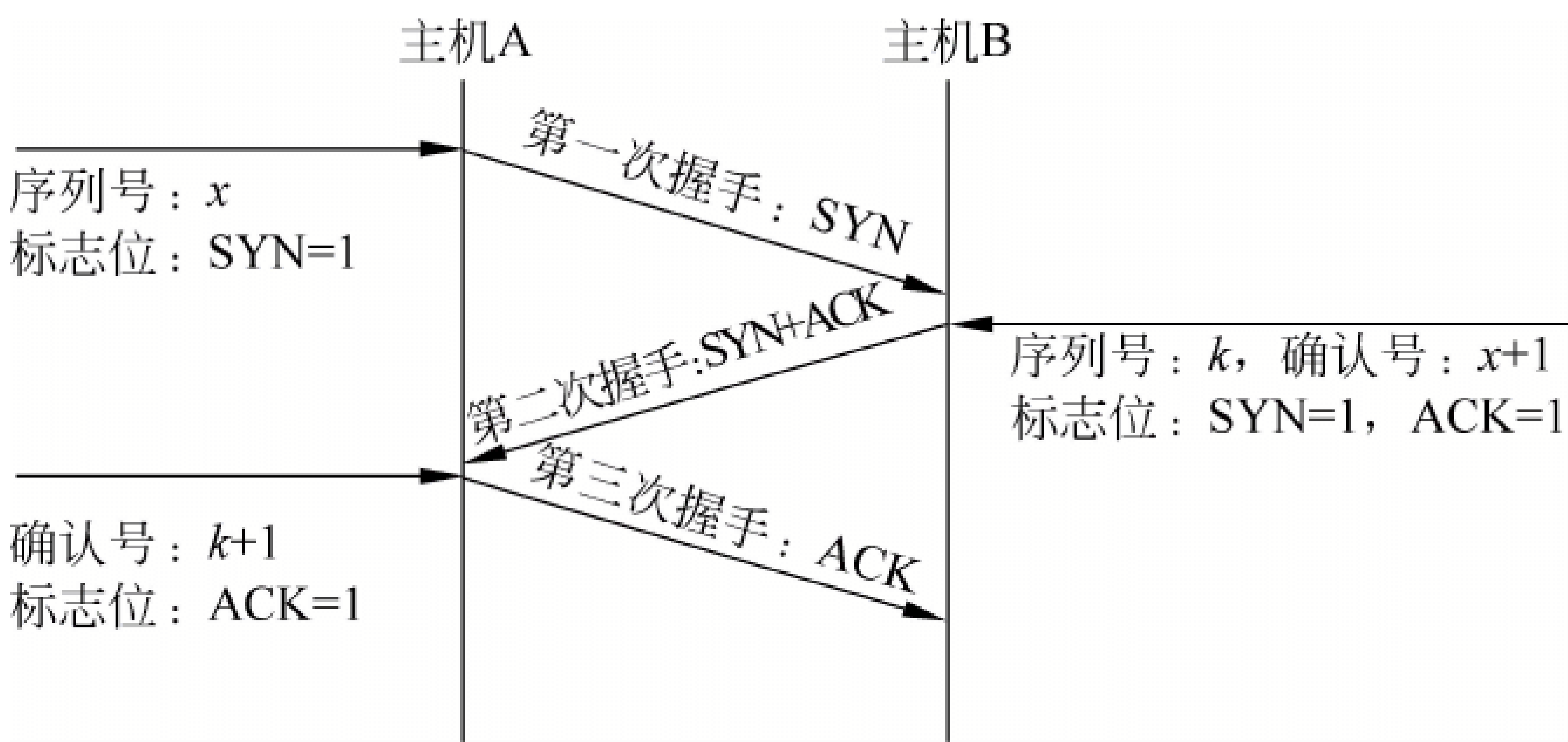



图 7-4　TCP 三次握手

第一次握手：建立连接时，主机 A 向主机 B 发送连接请求报文 SYN，这时报文首部中的同步位 SYN 置为 1，同时选择一个初始序列号 $x$，这时的 SYN 报文段不携带数据，但消耗掉一个序列号，主机 A 进入 SYN_SENT 状态，等待主机 B 确认。

第二次握手：主机 B 收到连接请求报文 SYN 后，如果同意建立连接，则向主机 A 发送确认报文。在确认报文中把 SYN 位和 ACK 位都置为 1，确认号为 $x+1$，同时选择一个初始序列号 $k$，确认报文也不能携带数据，并且消耗掉一个序列号，此时主机 B 进入 SYN_RCVD 状态。

第三次握手：主机 A 收到主机 B 的确认报文 SYN＋ACK，向主机 B 发送确认报文 ACK(ack$=k+1$)，此报文发送完毕，主机 A 和主机 B 进入 ESTABLISHED 状态，完成三次握手过程。主机 A 再发送一次确认报文，可以防止已失效的连接请求报文突然又传送到主机 B，因而产生错误。

完成三次握手后，主机 A 与主机 B 便建立起连接，开始传送数据。

**2. 四次挥手**

数据传输完毕后，要关闭连接。由于TCP连接是全双工的，因此每个方向都必须单独进行关闭。也就是当一方完成它的数据发送任务后就能发送一个FIN来终止这个方向的连接。收到一个FIN只意味着这一方向上没有数据流动，一个TCP连接在收到一个FIN后仍能发送数据。首先进行关闭的一方将执行主动关闭，而另一方执行被动关闭。这个过程被称为"四次挥手"，如图7-5所示。

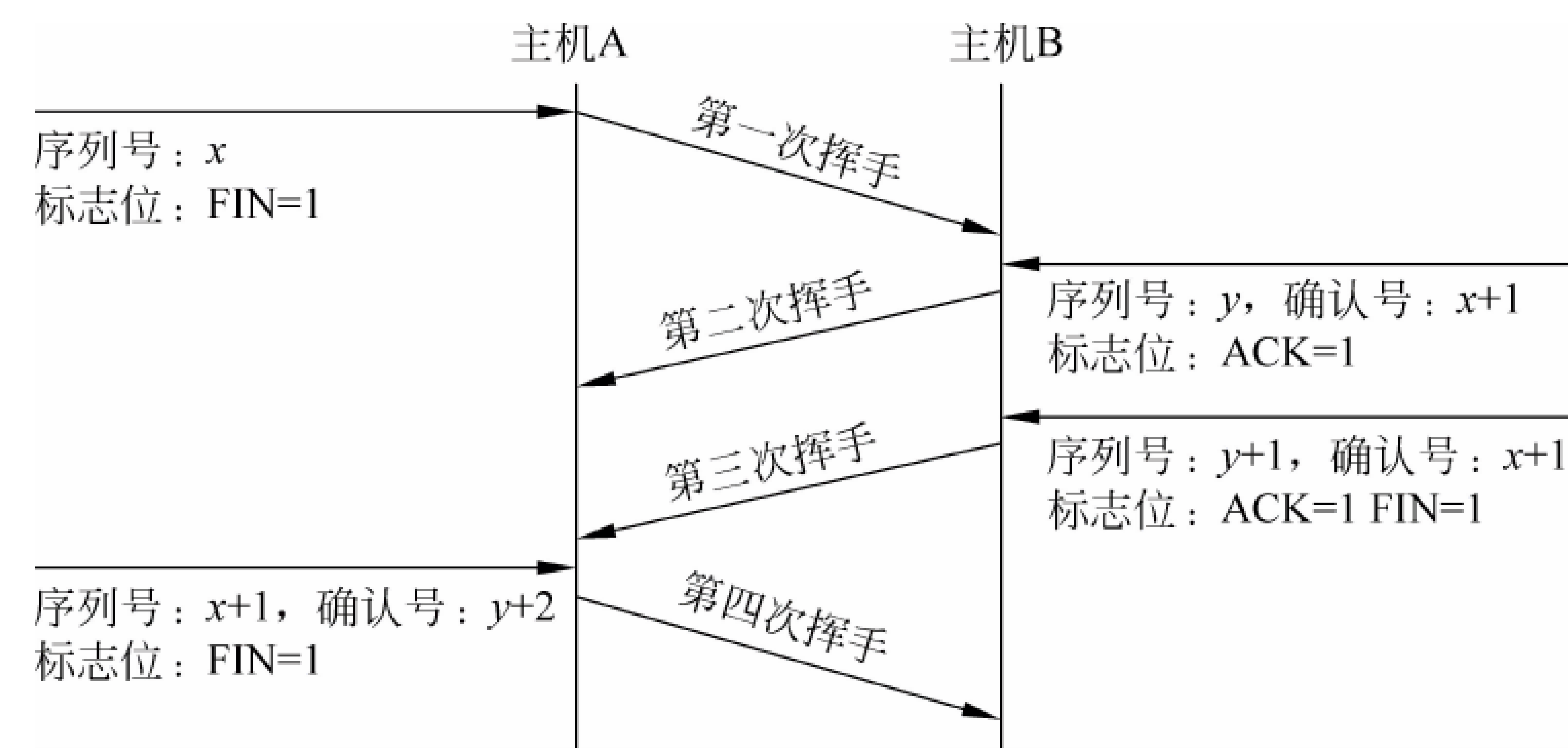



图7-5　TCP四次挥手

第一次挥手：主机A发送一个FIN报文，报文首部的FIN位置1，序列号为$x$，它等于前面已传送过的数据的最后一个字节的序号加1。FIN报文用来关闭主机A到主机B的数据传送。

第二次挥手：主机B收到这个FIN报文，向主机A发回一个ACK包（确认序号ACK=$x+1$，SYN=$y$，标志位ACK=1）。

第三次挥手：主机B向主机A发送一个FIN包（SYN=$y+1$，标志位ACK=1，FIN=1），关闭与客户端A的连接。

第四次挥手：主机A发回ACK报文确认，并将确认序号设置为$y+2$，即收到的报文序号加1。

至此，TCP连接拆除，可靠数据传输过程结束。

### 7.2.2 TCP窗口确认

通过上述对TCP三次握手过程的分析，我们知道主机使用数据段报头中的ACK确认在这个会话中已经接收到的数据字节；数据段报头序列号表明当前分段中包含的数据字节。TCP在发回源设备的数据段中使用确认号，指示接收设备期待接收的下一字节，该过程称为期待确认。

收到确认信息后，源设备即得知目的设备已收到数据流中确认号之前的所有字节，但不包括确认号所指示的字节。随后，源主机将继续发送数据段，且数据段的序列号应等于该确

认号。请记住，每个连接都实际包含两个单向会话，且两个方向上都在进行序列号和确认号的交换。

如图 7-6 中，左侧主机 A 正在向右侧主机 B 发送数据。它发送的数据段包含 10 字节的会话数据，数据段报头中的序列号等于 1。主机 B 接收数据段，并确认其序列号为 1，且数据字节数为 10，主机 B 随即向主机 A 发送数据段，确认收到数据。在确认数据段中，主机 B 将确认号设为 11，表明它期望下一接收数据的字节号为 11。当主机 A 接收到该确认信息时，它可以立即发送字节编号为 11 的下一会话数据段。

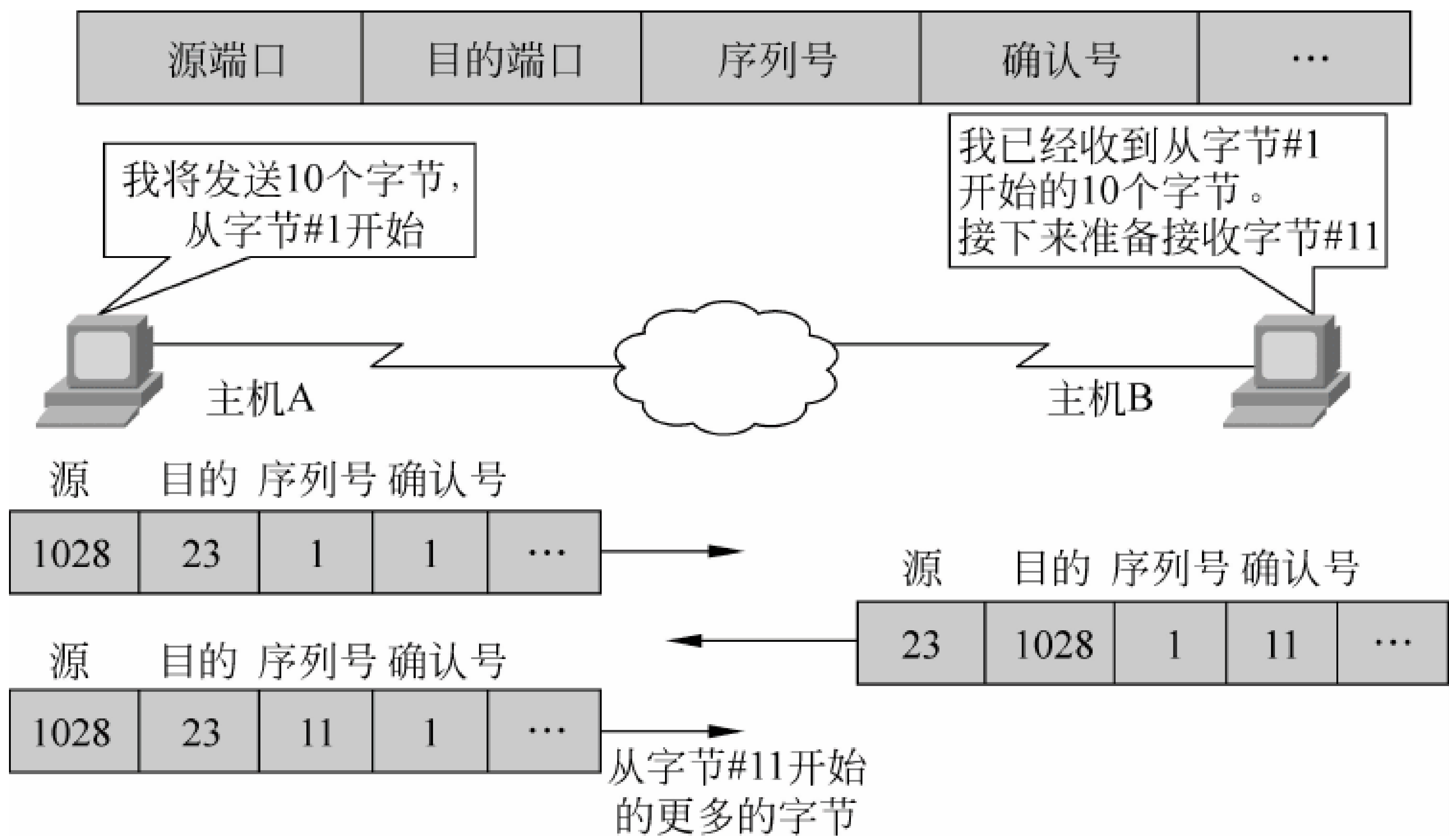



图 7-6　TCP 数据段的期待确认

在本例中，如果主机 A 需要等待每个 10 字节数据段的确认信息，网络将负担很多额外开销。为减少这些确认信息的开销，可以预先发送多个数据段，并在相反方向上采用单一 TCP 消息进行确认，即“TCP 窗口确认”。源主机在收到确认消息之前可以传输的数据大小称为窗口大小，窗口大小是 TCP 报头中的一个字段，用于管理流量控制。

例如当序列号从 1 算起时，如果已接收到 10 个 10 字节的数据段，则可以向源设备发送一条编号为 101 的确认消息，如图 7-7 所示。

### 7.2.3　TCP 数据重传

无论网络设计得如何完美，都可能发生数据丢失现象。因此，TCP 提供了管理数据段丢失的方法，其中一个方法就是重新发送未确认的数据。

使用 TCP 的目的主机服务通常只确认相邻序列的数据。如果一个或多个数据段丢失，只确认已完成数据流中的数据段。例如，如果接收到序列号为 1500 到 3000 以及 3400 到 3500 的数据段，那么确认号应为 3001，这是因为未收到序列号为 3001 到 3399 之间的数据段。如果源主机上的 TCP 未在规定时间内收到确认消息，它将根据收到的最后一个确认号重新发送数据。

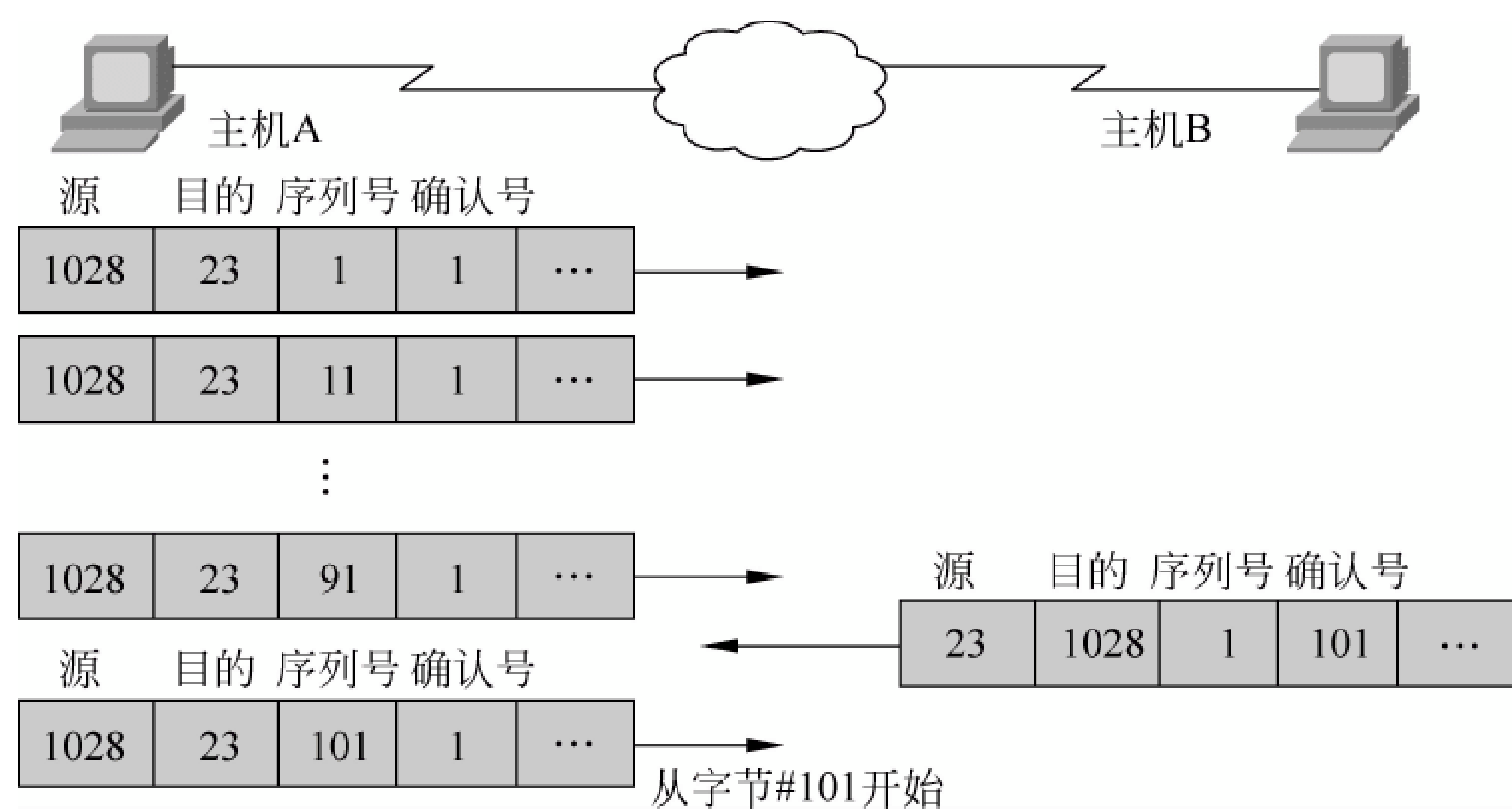



图 7-7 TCP 窗口确认

TCP 传输的标准流程是：主机传输数据段，并将数据段的副本列入重新发送队列，然后启动计时器。当接收到数据确认信息时，主机将从队列中删除对应数据段；如果到计时器超时还没有收到确认信息，将重新传输数据段。

主机还有一项备选功能，即选择性确认。如果两台主机都支持选择性确认功能，目的主机便可以确认间断数据段中的数据，那么源主机就只需要重新传输丢失的数据。

## 7.3 用户数据报协议 UDP

UDP 是一种简单协议，提供了基本的传输层功能。与 TCP 相比，UDP 的开销极低，因为 UDP 是无连接的，并且不提供复杂的重传、排序和流量控制机制。

### 7.3.1 UDP 的低开销与可靠性

UDP 数据报只需 8 字节报头，开销极低；并且 UDP 不像 TCP 那样提供重传、排序和流量控制机制等可靠性的功能。不过，这并不说明使用 UDP 的应用程序不可靠，而仅仅说明，作为传输层协议，UDP 不提供上述几项功能。如果需要这些功能，必须通过其他方式来实现。

某些应用程序可以容许小部分数据丢失（如网络游戏或 VoIP）。UDP 的典型应用是 Internet 广播，如果有一小段数据丢失，只是对广播的质量产生轻微的影响；而如果这些应用程序采用 TCP，那么将面临巨大的网络延迟，因为 TCP 需要不停检测数据是否丢失并重传丢失的数据。与丢失小部分数据相比，网络延迟对这些应用程序造成的负面影响更大。正是由于 UDP 的开销低，对此类应用程序非常有吸引力。

### 7.3.2 UDP 数据报重组

与 TCP 的通信机制不同，UDP 是无连接协议，因此通信发生之前不会建立会话。UDP

是基于事务的,换言之,应用程序要发送数据时,它仅是发送数据而已。

很多使用 UDP 的应用程序发送的数据量很小,用一个数据段就够了。但是也有一些应用程序需要发送大量数据,因此需要用多个数据段(严格来说,UDP 协议数据单元称为数据报(Datagram),尽管数据段和数据报可以互换使用来描述某个传输层协议数据单元)。

将多个数据报发送到目的主机时,它们可能使用不同的路径,到达顺序也可能跟发送时的顺序不同。与 TCP 不同,UDP 不跟踪序列号,UDP 不会对数据报重组,因此也不会将数据恢复到传输时的顺序,如图 7-8 所示。

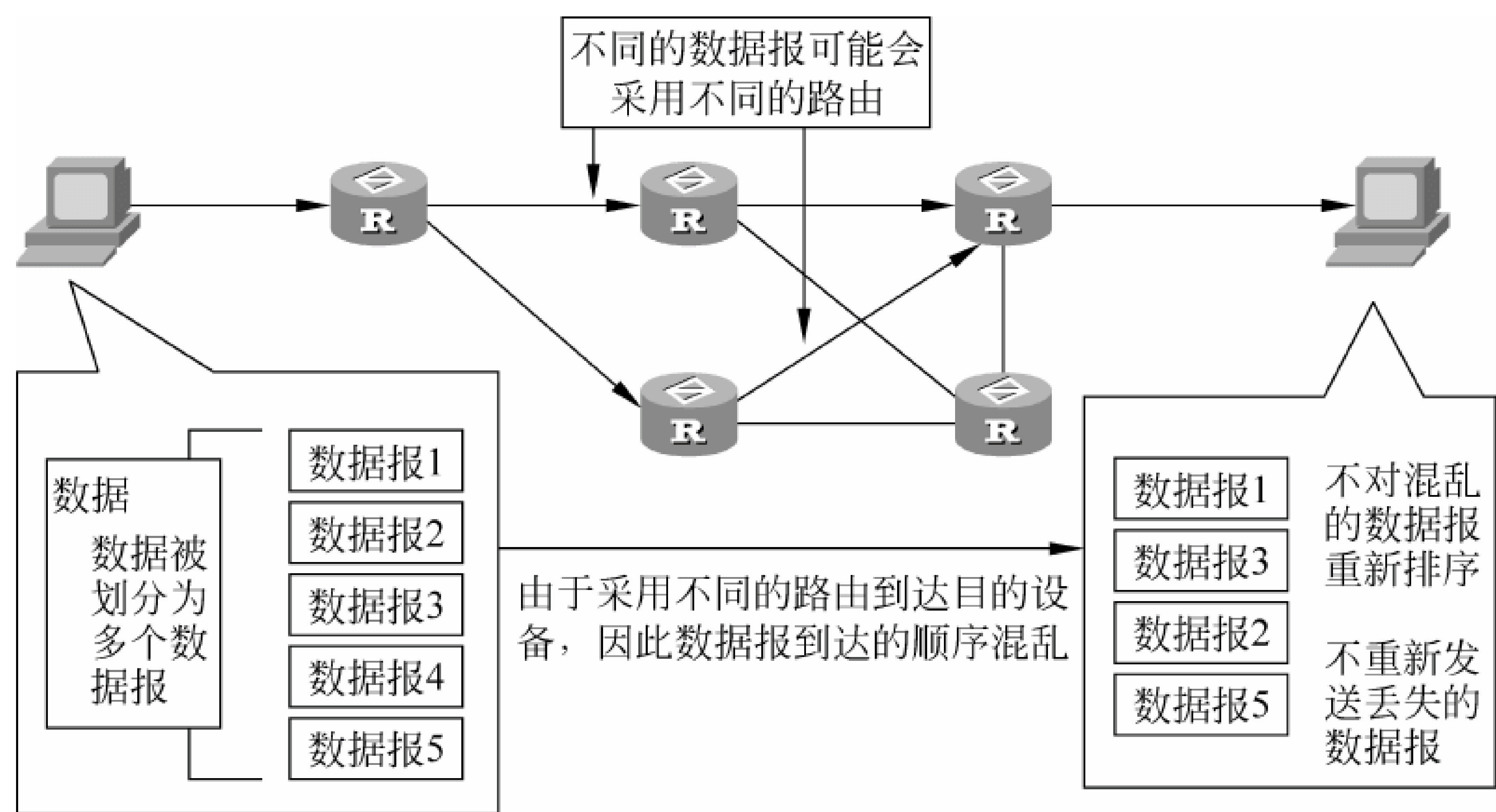



图 7-8　UDP 数据报重组

因此,UDP 仅仅是将接收到的数据按照先来后到的顺序转发到应用程序,如果数据的顺序对应用程序很重要,那么应用程序只能自己标志数据的正确顺序,并决定如何处理这些数据。

## 思考与练习

**一、填空题**

1. 传输层位于________和________之间,是第一个端到端的层次。

2. TCP/IP 协议簇中最常用的两种传输协议是________和________。

3. 传输层协议数据单元依靠其头部的________来识别不同的应用层数据。其中,________是本地主机上始发应用程序相关联的通信端口号;而________则是远程主机上目的应用程序相关联的通信端口号。

4. 公认端口也称知名端口,用于公共服务和应用程序。其范围是________。

5. TCP 在发回源设备的数据段中使用________指示接收设备期待接收的下一字节,该过程称为期待确认。

6. UDP 数据报只需________字节报头，开销极低；而 TCP 需要________字节报头，可以提供重传、排序和流量控制机制。

**二、选择题**

1. 以下知名端口不是 TCP 协议使用的是(　　)。

A. 20　　B. 21　　C. 23　　D. 69

2. 以下属于公认 TCP/UDP 常用端口的是(　　)。

A. 53　　B. 80　　C. 443　　D. 21

3. 以下不属于传输控制协议 TCP 特点的是(　　)。

A. 面向连接　　B. 可靠传输　　C. 确认重传　　D. 失序

4. 以下属于 UDP 协议特点的是(　　)。

A. 报头 8 字节　　B. 开销低，传输速度慢

C. 可以进行数据报重组　　D. 提供可靠传输

5. 以下(　　)不是 TCP 支持的应用层协议。

A. 文件传输协议 FTP　　B. 远程登录协议 Telnet

C. 简单邮件传输协议 SMTP　　D. 简单文件传输协议 TFTP

6. 以下(　　)不是 UDP 支持的应用层协议。

A. 路由信息协议 RIP　　B. 超文本传输协议 HTTP

C. 域名解析协议 DNS　　D. 简单文件传输协议 TFTP

**三、思考题**

1. 列举下列知名端口号的用途：20、21、23、25、69、80、110、194、443。

2. 简述 TCP 三次握手过程。

3. 简述传输层的两大协议各自的特点是什么？

第 8 章

# 网络操作系统简介

操作系统是计算机系统的重要组成部分，是计算机科学中一个重要研究领域。随着计算机应用的日益广泛，操作系统正在发生着巨大的变化，一个新的操作系统中往往汇集着计算机科学发展过程中的最新的科研成果与技术，也体现着现代计算机硬件技术的发展方向。可以说，操作系统是由客观需要而产生，并随着计算机应用的日益广泛和计算机技术的发展而逐渐发展并完善的。其功能由弱到强，人机交互由生硬到友好，应用领域由小变广。操作系统已经成为计算机系统的核心。

## 8.1 网络操作系统概述

### 8.1.1 操作系统概念

操作系统是介于计算机与用户之间的软件，是用于管理计算机硬件的。从用户的角度，操作系统的管理功能是不一样的。个人计算机操作系统应该是为用户提供友好的人机交互界面，方便用户使用计算机，而重视系统的使用效率；大型机的操作系统重点解决的是系统资源的利用率，而不十分重视人机交互的友好性；工作站的操作系统则兼顾了使用方便与效率；近年来移动计算设备开始流行，它的操作系统主要解决设备的可用性，以及容量有限的电池的管理。

从系统的角度，操作系统是系统资源的管理者。系统资源包括硬件资源和软件资源。操作系统管理着 CPU、内存空间、文件存储、I/O 设备等。操作系统面对许多甚至冲突的资源请求，如何高效而公平地分配资源成为重点研究的问题。

关于操作系统的定义，贝尔实验室的 Silberschatz 教授给出了一个定义：操作系统是一直运行在计算机上的程序（通常为内核），其他程序则为应用程序。

国内的专家学者则给出了一个更为全面的定义：操作系统是控制和管理计算机系统内各种硬件和软件资源、有效地组织多道程序运行的、在计算机中起最核心作用的软件，是用户和计算机之间的接口，使用户获得良好的工作环境，使计算机系统高效而自动化地运行。

### 8.1.2 操作系统的功能

设计操作系统的主要目的就是高效地管理计算机系统资源，为用户提供友好的人机界面。

**1. 处理器管理**

处理器(CPU)是计算机系统的核心。为了提高 CPU 的利用效率,操作系统采用多道程序技术和进程的概念。当一个程序因等待一个条件而不能运行时,就把处理器占用权交给另一个可运行程序;或者当一个比当前运行的程序更重要更高级别的程序出现时,也要把处理器的占用权交给那个程序。处理器管理就是实施分配调度策略对处理器进行分配和回收,以充分地利用 CPU 资源。

**2. 存储管理**

存储器是计算机系统中用户作业和进程的存储环境。充分利用存储器,必要时从逻辑上扩充内存是操作系统必须解决的问题。操作系统在存储管理中的主要任务是:内存空间的分配、内存保护、内存回收、内存扩充和内存优化等。

**3. 设备管理**

设备是指计算机系统中的输入/输出设备,因为涉及众多的实际的物理设备,所以设备管理是操作系统中最庞杂琐碎的部分。操作系统的主要任务就是完成用户提出的 I/O 请求,为用户分配 I/O 设备;提高 CPU 和 I/O 设备的利用率;方便用户使用 I/O 设备。

**4. 文件管理**

计算机中的信息资源都以文件方式存储在计算机的外存中。如何有效地组织管理这些文件是操作系统必须解决的问题,文件管理的功能包括文件的存储、检索、修改、共享、保密和保护等操作。一般操作系统都有一个功能强大的文件系统。

**5. 人机交互界面**

操作系统为用户提供了人机交互界面,以方便用户工作。典型的界面有:

(1) 命令行方式。如 MS-DOS 和 UNIX,用户通过在提示符后输入命令调用系统服务、执行程序。

(2) 窗口界面。随着计算机性能的提高,很多操作系统都提供了图形化的窗口界面,用户感觉比较直观方便。

### 8.1.3 网络操作系统的功能

操作系统根据不同的分类标准分为很多种类,比如批处理操作系统、分时操作系统、实时操作系统、个人计算机操作系统、网络操作系统、分布式操作系统等。网络操作系统(Network Operating System, NOS)是操作系统中的一个重要分支,是基于计算机网络的、在各种计算机操作系统之上按网络体系结构协议标准设计开发的软件,它包括网络管理、通信、安全、资源共享和各种网络应用。网络操作系统把计算机网络中的各个计算机有机地连接起来,其目标是相互通信及资源共享。

网络操作系统要具有开放性,只有遵循国际规范,才能和其他系统相互兼容,方便互连互通;网络操作系统要具有一致性,即底层向高层提供一致性的服务接口,即一致的命令类型、命令的内部参数及合法的访问命令序列等;另一方面,操作系统要具有透明性,即用户

只要知道他应该得到什么样的服务，而不需要知道服务的实现细节和所需资源。

网络操作系统的功能主要有如下几方面。

1）网络通信

提供通信双方之间无差错的、透明地进行数据传输，主要包括建立和拆除通信链路，对传输中的分组进行路由选择和流量控制，传输数据的差错检测和纠错，这些功能通常由链路层、网络层和传输层的硬件，以及相应的网络软件共同完成。

2）网络服务

直接面向最终网络用户提供的服务，主要包括：电子邮件服务、文件传输、存取和管理服务、共享硬盘服务、共享打印服务等。

3）网络管理

网络管理最主要的任务是安全管理，一般这是通过“存取控制”来确保存取数据的安全性；以及通过“容错技术”来保证系统故障时数据的安全性。此外，还包括对网络设备故障进行检测，对使用情况进行统计，以及为提高网络性能和安全而提供必要的信息。

4）提供网络接口

向用户提供一组方便有效统一、取得网络服务的接口以改善用户界面。如命令接口、菜单、窗口等。

### 8.1.4　网络操作系统的工作模式

根据网络工作方式和所使用操作系统的不同，局域网可分为对等模式、专用服务器模式和客户/服务器模式三种类型。

**1. 对等模式**

对等模式(Peer to Peer，P2P)网络就是在一个网络中不需要专用的服务器，每一台接入网络的计算机既是服务器也是工作站，拥有绝对的自主权。同时，不同的计算机之间可以实现互访，进行文件的交换和资源共享。

对等是指网络的工作方式，与网络拓扑之间没有直接关系。在对等网中没有专用的服务器，每一台计算机的身份是由该计算机在某一时间所扮演的角色来确定的，当该计算机提供可共享的资源给网络中的其他计算机时就扮演服务器的角色，而需要访问网络中其他计算机上的共享资源时便充当工作站的角色。在对等网中不需要使用像网络中 Windows 2000 Server、UNIX 等专门的网络操作系统，由于像 Windows 98、Windows NT Professional、Windows 2000 Professional、Windows Me、Windows XP 等常用的桌面操作系统中已内置了基本的网络通信功能，所以可以很方便地使用这些操作系统来组建对等网。

对等网具有以下优点：

(1) 组建和维护容易，不需要专用的服务器。

(2) 可实现低价格组网，使用简单。

对等网具有以下缺点：

(1) 数据的保密性差。

(2) 文件的存放分散。

**2. 专用服务器模式**

专用服务器(Server-Based)模式的特点是网络中必须有一台专用文件服务器，而且所有的工作站都必须以服务器为中心，工作站与工作站之间无法直接进行通信。当工作站之间进行通信时，需要通过服务器作为中介，工作站端进行文件读取和数据传输时都需要服务器的参与。NetWare 网络操作系统是工作于专用服务器结构的代表。

专用服务器模式具有以下的优点：

(1) 数据的保密性很强。

(2) 可以严格地对每一个工作站用户设置访问权限，可靠性强。

专用服务器模式存在以下的缺点：

(1) 网络工作效率较低，网络的安装和维护较困难。

(2) 工作站上软硬件资源无法实现共享。

**3. 客户/服务器模式**

客户/服务器(Client/Server)模式是继专用服务器结构之后产生和发展起来的。主从式结构解决了专用服务器结构中存在的不足，客户端既可以与服务器端进行通信，同时客户端之间也可进行直接对话，而不需要服务器的中介和参与。Windows NT Server、Windows 2000 Server、Windows Server 2003 网络操作系统是工作于客户/服务器模式网络中的典型代表。

客户/服务器模式具有以下的优点：

(1) 可以有效地利用各工作站端的资源。

(2) 可以减少服务器上的工作量，网络的工作效率较高。

客户/服务器模式具有以下的缺点：

(1) 对工作站的管理较为困难。

(2) 数据的安全性低于专用服务器模式。

# 8.2 网络操作系统简介

## 8.2.1 UNIX 操作系统

UNIX 操作系统是由美国电话及电报公司(American Telephone & Telegraph, AT&T)的贝尔实验室于 1969—1970 年研制出来的一种多用户、多任务网络操作系统。因为 UNIX 操作系统大部分代码都是用 C 语言写的，所以其移植性比较好。1978 年，加利福尼亚大学伯克利分校推出了 UNIX 的一种新的版本，即“1 BSD(1st Berkeley Software Distribution)”，开创了 UNIX 的另一个分支——BSD 系列。同一时期，AT&T 将 UNIX 变成商业化的产品。从此，BSD 的 UNIX 便和 AT&T 的 UNIX 分庭抗争，UNIX 就分为

System Ⅳ和 4.x BSD 这两大主流。

随着 UNIX 的发展，出现了一些其他商业化的版本，主要有 IBM 的 AIX，Sun 公司的 Solaris，HP 公司的 HP-UX，微软公司的 XENIX，硅谷图形公司（Silicon Graphics，SGI）的 IRIX 等。UNIX 是目前功能最强大、安全性最高的网络操作系统。

UNIX 向用户提供两种界面——用户界面和系统调用。UNIX 的传统界面是基于文本的命令行界面，即 Shell。另一种就是图形用户界面，可以利用鼠标、菜单、窗口等图形化界面进行操作，这种方式比较直观友好。

### 8.2.2　Linux 操作系统

Linux 是以 UNIX 为基础而开发的一个操作系统。1991 年芬兰赫尔辛基大学的一名叫 Linus Torvalds 的学生，在 Minix（一种类 UNIX 的小型操作系统）的基础上开发了一种基于 Intel X86 平台的操作系统，它具有 UNIX 的全部功能。1991 年 10 月 5 日发布了 Linux0.0.2 版本，并以可爱的企鹅作为标志。随后，他把源代码发布在 Usenet 新闻组上，并邀请所有有兴趣的人发表评论或者共同修改代码。在 Linux 社区的共同努力下，1994 年 3 月，Linux 1.0 版本被发布，这是一个功能完善、稳定可靠的操作系统。Linux 最大的特点在于其源代码是向用户开放的，任何一个用户可根据自己的需要修改 Linux 的内核，并发布新的版本。Linux 的特点如下。

**1. 多用户多任务**

Linux 支持多个用户从相同或不同的终端上同时使用一台计算机（多用户），在同一时间段内，Linux 系统能响应多个用户的不同请求，也可以在 Linux 中同时执行多个程序（多任务）。

**2. 高度的稳定性**

Linux 的内核继承了 UNIX 的优良特性，可以长期高效、稳定地运行。Linux 不易受蠕虫攻击，到目前为止，只有屈指可数的几种病毒感染 Linux，这主要归功于 Linux 的基础架构的健壮性。Linux 的基础架构由相互无关的层组成，每层都有特定的功能和严格的权限许可，从而保证 Linux 最大地稳定运行。

**3. 良好的兼容性**

Linux 遵循 POSIX（Portable Operating System Interface of UNIX，可移植操作系统接口）标准，所以 Linux 与现在的 System Ⅴ以及 BSD 等主流 UNIX 系统均兼容，在 UNIX 下的可执行程序，也几乎完全可以在 Linux 上运行。

**4. 强大的可移植性**

由于 Linux 的系统内核只有不到 10%的源代码用汇编语言编写，其余均是采用 C 语言编写，因此其可移植性很强。它可以运行在 PC、移动计算设备、小型机、中型机甚至大型机上。迄今为止，Linux 是支持硬件平台最多的操作系统。

**5. 支持多种文件系统**

Linux 支持多种文件系统，可以把多种文件系统以挂载（Mount）的方式加入。例如，

Windows 98 平台下的 FAT16/32、Windows NT/2000 下的 NTFS、OS2 下的 HPFS、网络上其他计算机共享的文件系统 NFS(Network File System)等都是 Linux 支持的系统。

**6. 完善的网络功能**

Linux 继承了 UNIX 作为网络操作系统的优点，使用 TCP/IP 作为默认的网络通信协议，并且内置了许多服务软件，如 Web 服务器——Apache、FTP 服务器——Vsftpd、邮件服务器——Sendmail、网络防火墙——Iptables、DNS 服务器——BIND 等。

由于 Linux 内核可以自由获得，并允许厂商自行搭配其他应用软件，开发相关的管理工具，形成 Linux 的不同发行版本。目前，Linux 的发行版本不下 300 种，其中影响较大的如下。

Red Hat：全世界 Linux 用户最熟悉的一个发行版本，其产品分为收费的 Red Hat Enterprice Linux(RHEL)和免费的 Fedora Core，前者主要用于服务器，后者主要用于桌面系统。因 CentOS 是 RHEL 的克隆版，且免费，也有不少用户使用 CentOS 版本。

Debian：可以算是最遵守 GNU 规范的 Linux 发行版，拥有强大的 apt-get 软件包管理工具，安装、升级软件比较容易。

Ubantu：是基于 Debian 的 Linux 发行版，安装方便，对硬件的支持较好。每年的 4 月和 10 月发布新的版本。

SUSE：是德国著名的发行版本，后被 Novell 公司收购，是一个专业优秀的发行版本。

### 8.2.3 NetWare 操作系统

NetWare 是 Novell 公司推出的高性能的局域网操作系统，它也是一个多用户、多任务的网络操作系统，它使用开放协议技术使不同类型的工作站可以与公共服务器通信，这种技术满足了广大用户在不同种类网络间相互通信的要求，能把各种网络协议紧密地连接在一起，方便与各种大中小型机通信。NetWare 对硬件的要求比较低(工作站只要 286 机器就可以)，因而受到一些设备比较落后的中小企业的欢迎。目前，这种操作系统的市场占有率呈下降趋势，它的市场份额被 Windows 系列和 Linux 系统瓜分。

### 8.2.4 Windows 网络操作系统

Windows 系列网络操作系统是微软开发的一种界面友好、操作简便的网络操作系统。Windows 网络操作系统主要包括 Windows NT、Windows 2000 Server、Windows 2003 Server、Windows 2008 Server 等。Windows 系列网络操作系统具有以下特点：

- 直观高效的面向对象的图形用户界面，易学易用。
- 用户界面统一，友好、美观。
- 丰富的设备无关的图形操作。
- 多任务。
- 支持对称多处理结构，支持多线程并行，支持多种网络协议和多文件系统。
- 丰富的 Windows 软件开发工具。

# 8.3 Windows Server 2008 简介

## 8.3.1 Windows Server 2008 的特点

Windows Server 2008 是微软新推出的新一代网络操作系统，它秉承了 Windows 操作系统简单易用的风格，成为中小企业应用服务器的首选。Windows Server 2008 代表了下一代网络操作系统，它在实用性、安全性和可操作性方面都有了极大的飞跃。它可以充分地发挥服务器的硬件性能，为企业网络提供更高效的网络传输和更可靠的安全性；不仅降低了网络管理员的负担，而且提高了工作效率。与以往的网络操作系统相比，它具有以下特点。

**1. 更加易用**

Windows Server 2008 的易用性主要体现在两个方面：

(1) 安装过程更加友好。Windows Server 2008 安装过程基本是在一个图形用户界面的环境下完成的，并且完成了大部分初始化工作。从安装到能够正常使用，整个过程大约需要十几分钟的时间，在这个过程中唯一需要输入的信息就是产品的密钥，而其他需要设置的信息在 Windows 2008 中已经完全消失，这样大大加快了整个安装流程。

(2) 拥有强大统一的服务器管理控制台。Windows Server 2008 的服务器管理控制台进行了进一步的升级强化，除了能让管理员添加服务器角色和配置服务器的细节外，新的服务器管理控制台还允许配置时间和时区、设定 Windows Update 等其他一些在过去的安装过程中弹出来的问题，大大减少了手动安装系统的时间。统一的管理控制台呈现了一个清晰的服务器配置界面，你可以随意地配置服务器的各种应用，Web 服务、DHCP 服务、DNS 服务等。

**2. 强大的虚拟化技术**

虚拟化是 Windows Server 2008 的一个重大创新功能，这一技术可以有效减少企业的总体成本。Windows Server 2008 融合了 Intel 和 AMD 两家公司的虚拟化技术，从而提供虚拟硬件支持平台，而这是其他虚拟化软件难以做到的。Windows Server 2008 的虚拟化技术能"创建"许多的虚拟服务器，这样可以最大限度地发挥软硬件的作用。我们可以在一台性能强劲的服务器上运行多个服务器软件平台，这将使系统更加可靠，消耗的功率更低并且占用的空间更少。Windows Server 2008 虚拟化技术的一大目标就是加强闲置资源利用，减少浪费。

**3. 增强的保护**

Windows Server 2008 提供了一系列新的和改进的安全技术，这些技术增强了对操作系统的保护，为企业的运营和发展奠定了坚实的基础。Windows Server 2008 通过网络访

问保护系统(Network Access Protection,NAP),使得企业的个人计算机必须完成一系列的管理性测试和任务,否则是不能连接到网络的。

Bit Locker 在多个驱动器上进行完整卷加密,为数据提供额外的安全保护,甚至当系统处于未经授权操作或运行不同的操作系统时也能提供安全保护。

Windows Server 2008 中的高级安全防火墙有了较大的改进,它不但支持双向保护,即可以对出站、入站进行过滤,而且它将 Windows 防火墙功能和 Internet 协议安全(IPSec)集成到一个控制台中。使用这些高级选项可以按照环境所需的方式配置密钥交换、数据保护(完整性和加密)以及身份验证设置。

只读域控制器(Read-Only Domain Controller, RODC):这是 Windows Server 2008 操作系统中的一种新型域控制器配置,使组织能够在域控制器安全性无法保证的位置轻松部署域控制器。RODC 维护给定域中 Active Directory 目录服务数据库的只读副本。通过将只读 Active Directory 数据库副本放置在更接近分支办公室用户的地方,这些用户可以更快地登录,并能更有效地访问网络上的身份验证资源。

### 8.3.2 Windows Server 2008 的版本

Windows Server 2008 已经发布了多个版本,不同的版本定位于不同的市场,以满足不同企业的需求,从小企业到分布于全球的大型分布式企业。这些版本包括标准版、企业版、数据中心版、Web 服务器版、安腾版、高性能计算版等。

标准版(Windows Server 2008 Standard)是迄今最稳固的 Windows Server 操作系统,其内置的强化 Web 和虚拟化功能,是专为增加服务器基础架构的可靠性和弹性而设计,亦可节省时间及降低成本。其利用功能强大的工具,拥有更好的服务器控制能力,并简化设定和管理工作;而增强的安全性功能则可强化操作系统,以协助保护数据和网路,并可为企业提供扎实且可高度信赖的基础。32 位版最大可支持 4GB 内存和 4 路处理器,64 位版最大支持 64GB 的内存。

企业版(Windows Server 2008 Enterprise)可提供企业级的平台,部署企业关键应用。其所具备的群集和热添加(Hot-Add)处理器功能,可协助改善可用性,而整合的身份管理功能,可协助改善安全性,利用虚拟化授权权限整合应用程序,则可减少基础架构的成本,因此 Windows Server 2008 Enterprise 能为高度动态、可扩充的 IT 基础架构,提供良好的基础。32 位版支持 8 路处理器和 64GB 内存;64 位版支持最高 2TB 内存。企业版支持更大规模的网络,更多的用户,更复杂的网络应用。

数据中心版(Windows Server 2008 Datacenter)所提供的企业级平台,可在小型和大型服务器上部署具企业关键应用及大规模的虚拟化。其所具备的群集和动态硬件分割功能,可改善可用性,而通过无限制的虚拟化许可授权来巩固应用,可减少基础架构的成本。此外,此版本亦可支持 2 到 64 颗处理器,因此 Windows Server 2008 Datacenter 能够提供良好的基础,用以建立企业级虚拟化和扩充解决方案。

Web服务器版(Windows Web Server 2008)是特别为单一用途Web服务器而设计的系统,整合了重新设计架构的IIS 7.0、ASP.NET和Microsoft .NET Framework,以便提供任何企业快速部署网页、网站、Web应用程序和Web服务。

安腾版(Windows Server 2008 for Itanium-Based Systems)已针对大型数据库、各种企业和自订应用程序进行优化,可提供高可用性和多达64颗处理器的可扩充性,能符合高要求且具关键性的解决方案的需求。

高性能计算版(Windows HPC Server 2008)是下一代高性能计算(High Performance Computing,HPC)平台,可提供企业级的工具给高生产力的HPC环境,由于其建立于Windows Server 2008及64位元技术上,因此可有效地扩充至数以千计的处理器,并可提供集中管理控制台,协助主动监督和维护系统健康状况及稳定性。其所具备的灵活的作业调度功能,可让Windows和Linux的HPC平台间进行整合,亦可支持批量作业以及服务导向架构(Service-Oriented Architecture,SOA)工作负载,而增强的生产力、可扩充的性能以及使用容易等特色,则可使Windows HPC Server 2008成为同级中最佳的Windows环境。

## 8.3.3 Windows Server 2008 基本设置

### 1. 配置服务器的IPv4地址

网络服务器通常使用固定IP地址,该IP地址由网络管理员统一规划分配。这里使用TCP/IPv4来配置Windows Server 2008服务器,具体配置步骤如下。

步骤1:依次选择"开始"→"控制面板"→"网络和共享中心",打开如图8-1所示"网络和共享中心"窗口,单击"本地连接"右侧的"查看状态",打开"本地连接状态"窗口。




图8-1　打开网络和共享中心

步骤 2：如图 8-2 所示，单击“本地连接状态”窗口中的“属性”按钮。

步骤 3：在如图 8-3 所示的“本地连接属性”窗口中，选择“Internet 协议版本 4(TCP/IPv4)”，然后，单击“属性”按钮。

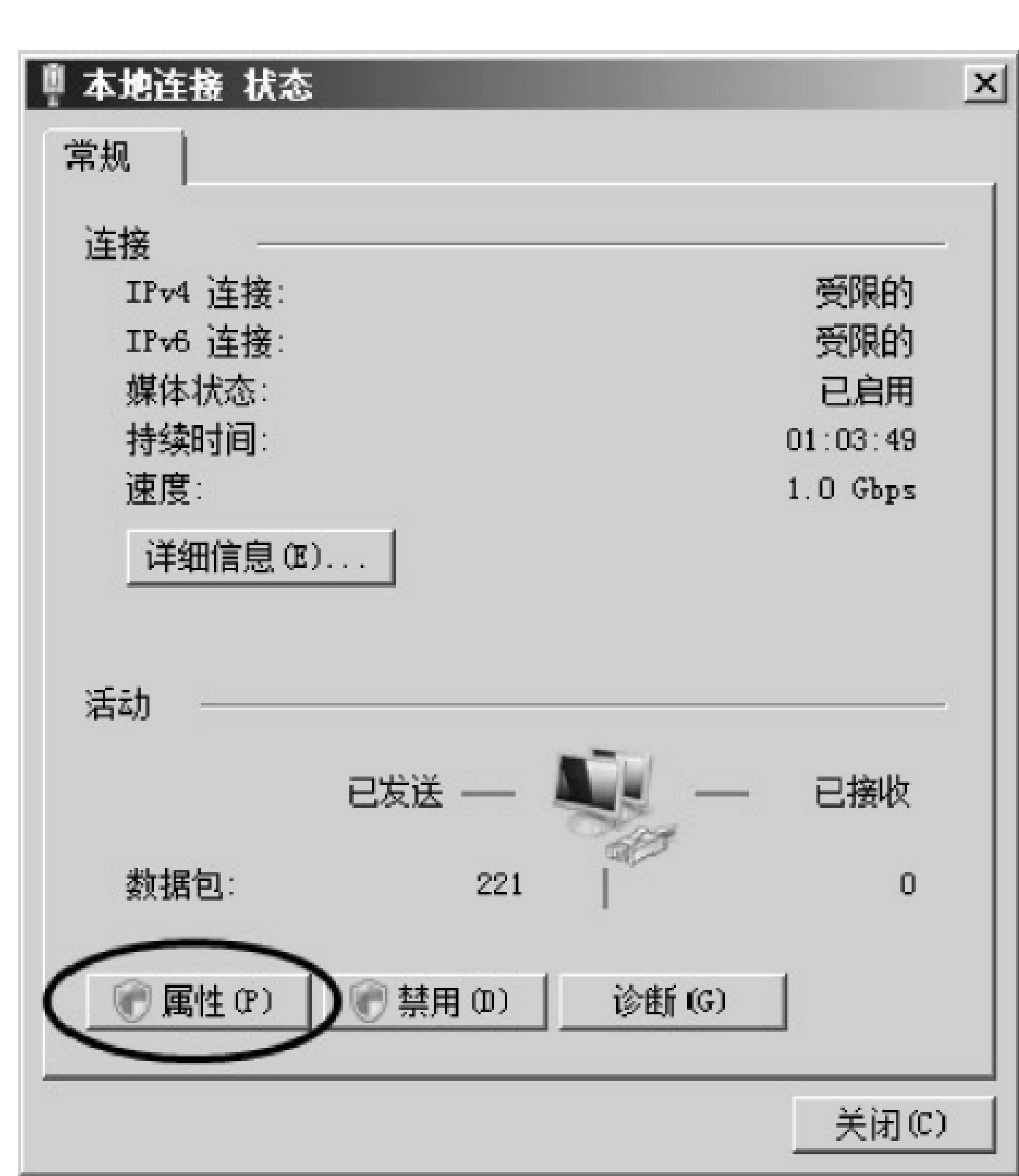



图 8-2 本地连接状态

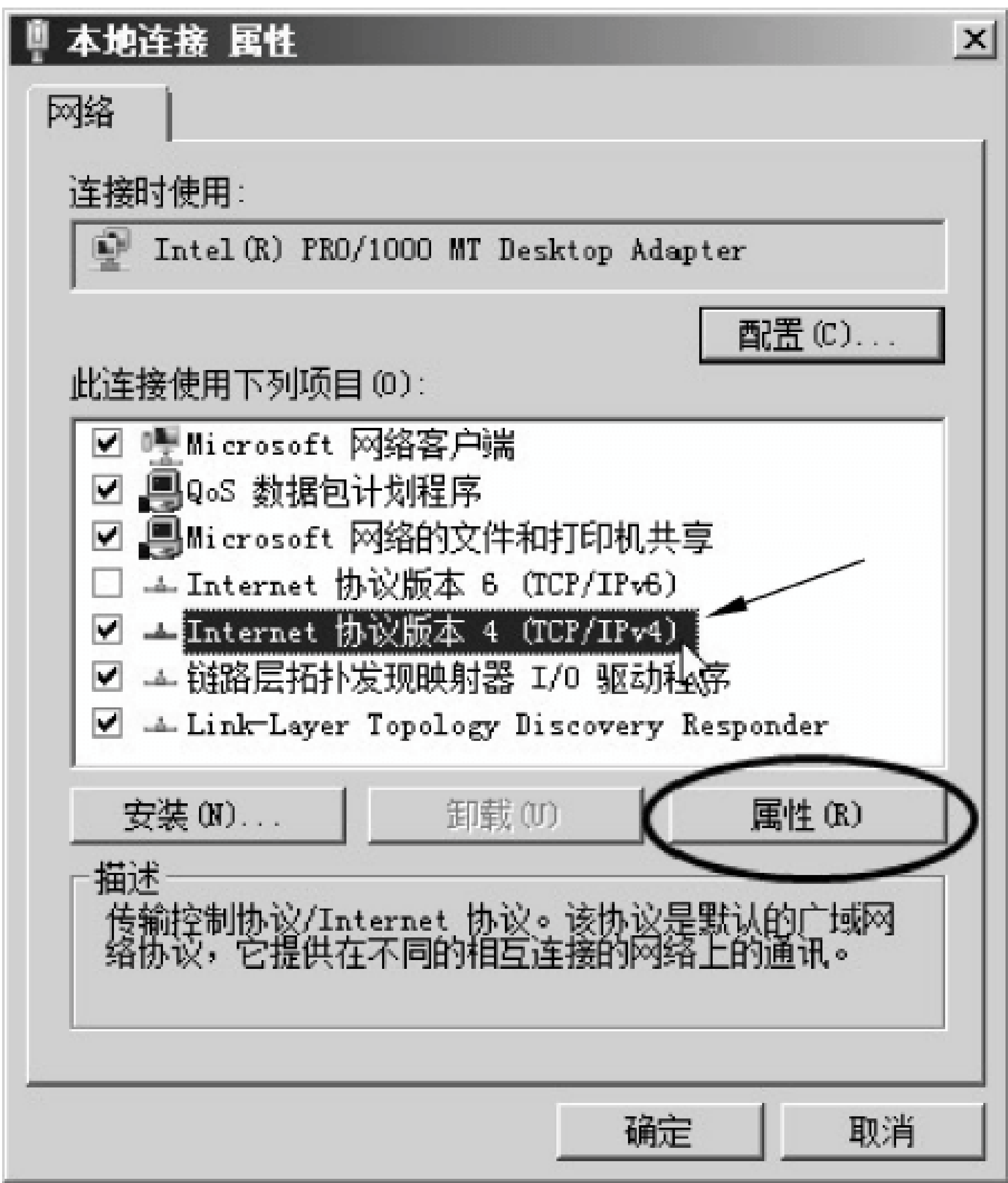



图 8-3 本地连接属性

步骤 4：在如图 8-4 所示的“Internet 协议版本 4(TCP/IPv4)属性”窗口中，选择“使用下面的 IP 地址”，分别输入“IP 地址”、“子网掩码”、“默认网关”等内容。选择“使用下面的 DNS 服务器地址”，输入“首选 DNS 服务器”和“备用 DNS 服务器”值。

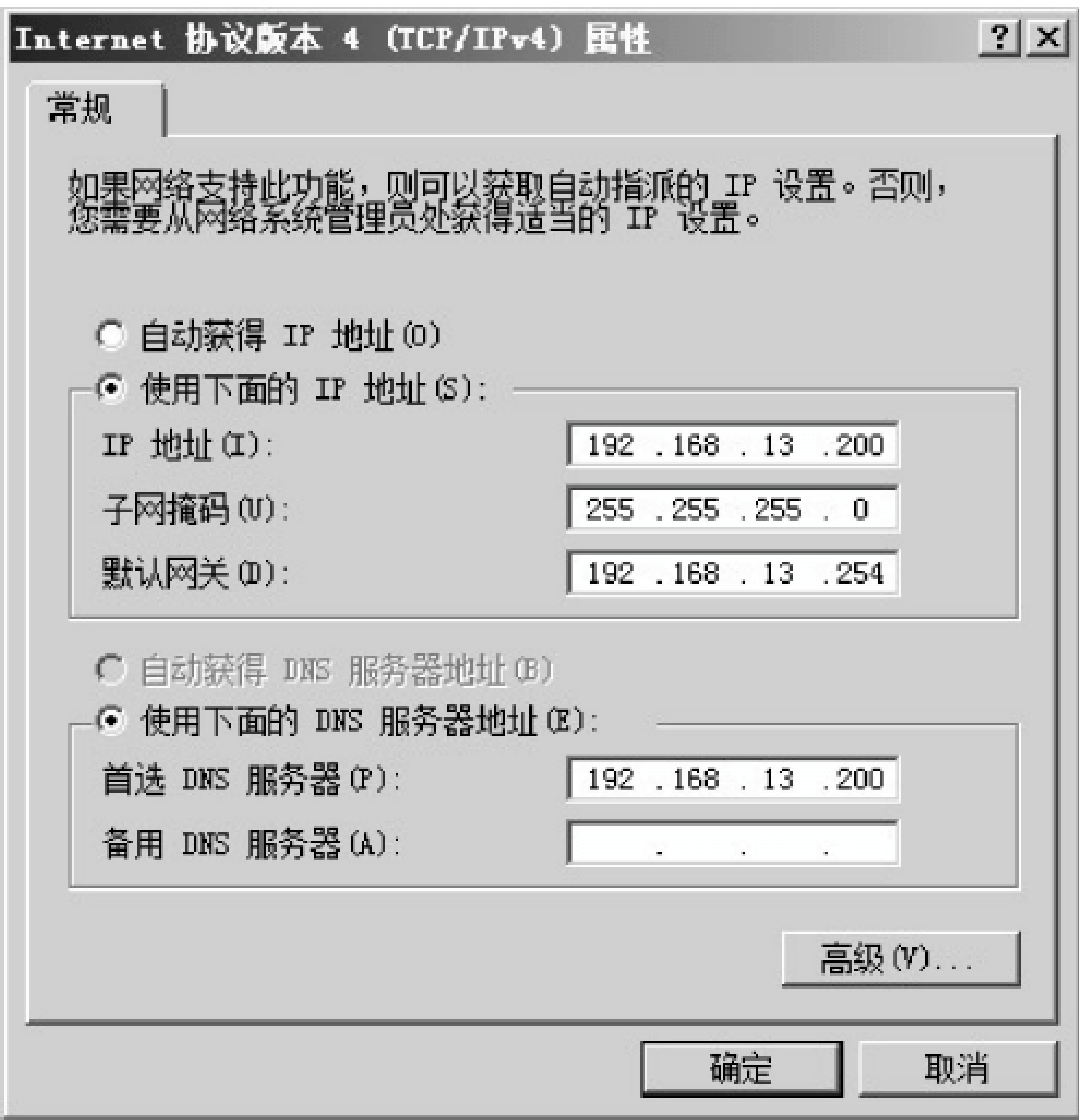



图 8-4 TCP/IPv4 属性设置

### 2. 设置服务器名称

步骤 1：依次选择“开始”→“管理工具”→“服务器管理器”，打开如图 8-5 所示“服务器管理器”窗口。单击“更改系统属性”，打开如图 8-6 所示“系统属性”窗口。




图 8-5　更改系统属性

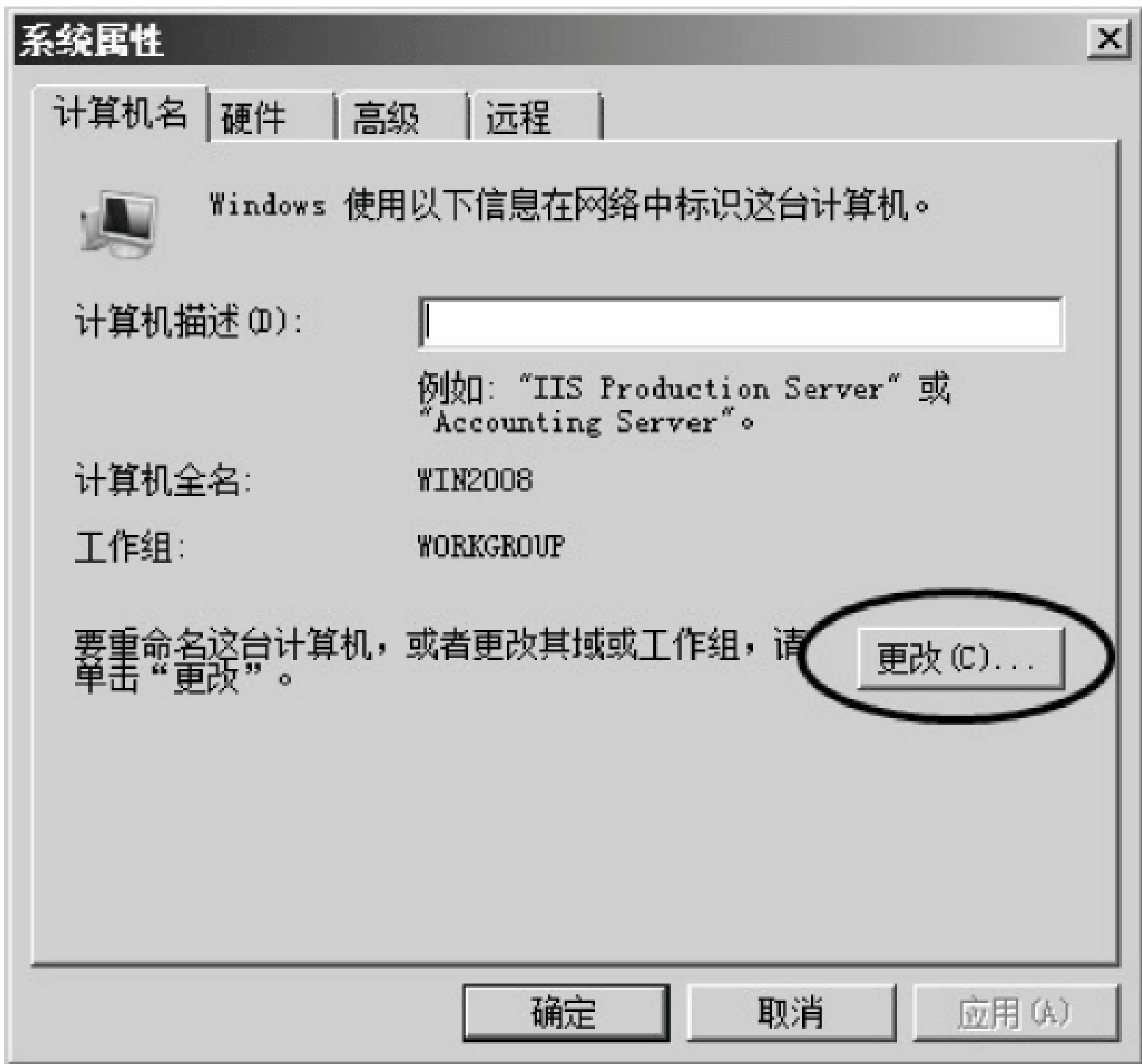



图 8-6　“系统属性”窗口

步骤 2：在“系统属性”窗口中，单击“更改”按钮。打开如图 8-7 所示“计算机名/域更改”窗口。

步骤 3：在“计算机名/域更改”对话框的“计算机名”文本框中，输入新的计算机名，单击“确定”按钮，然后重启服务器就可以了。

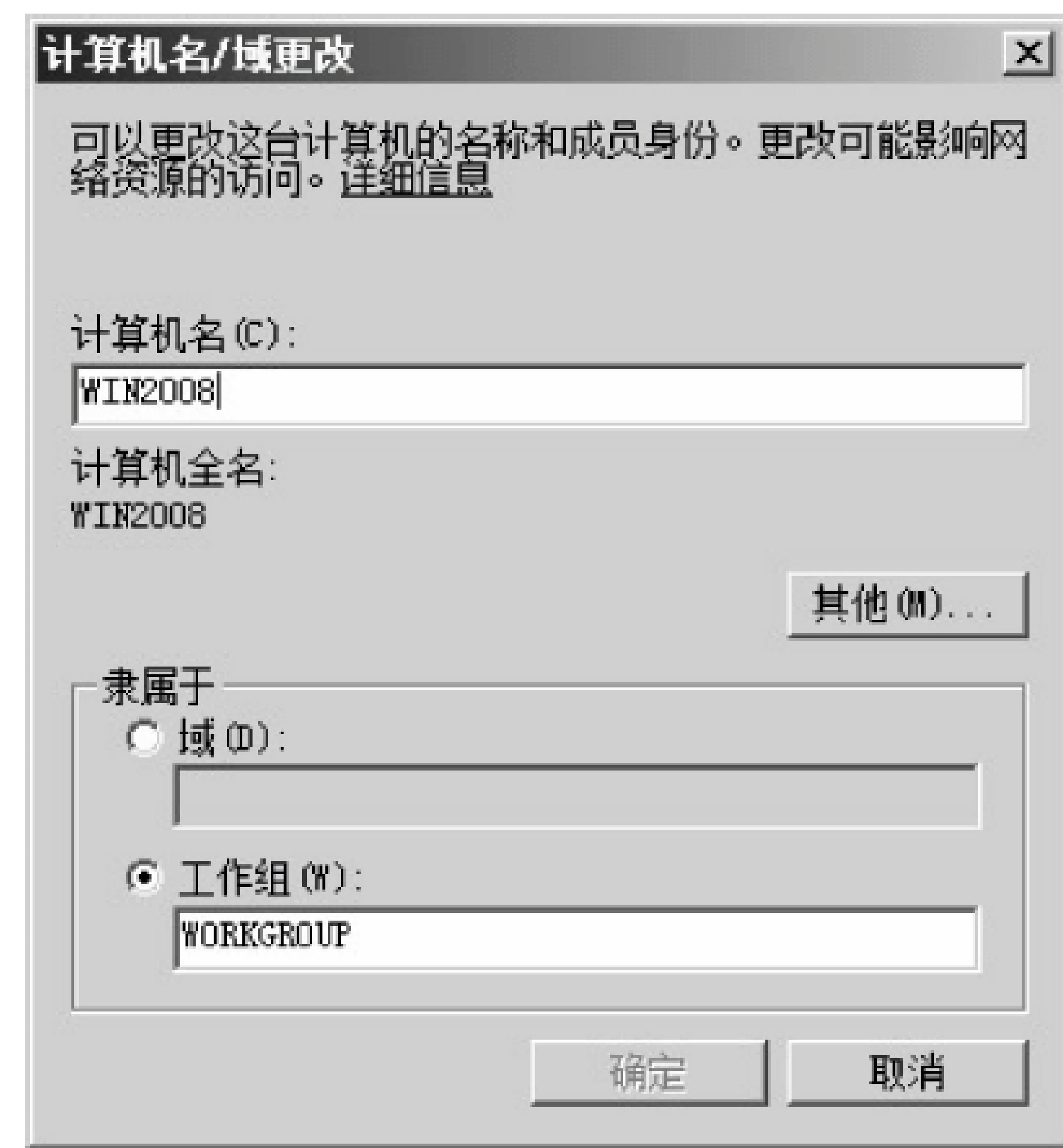



图 8-7 更改计算机名称

### 3. 关闭服务器防火墙

微软的 Windows 操作系统以前也内置了防火墙,但防火墙的功能比较弱,很多系统管理员将其视为鸡肋,它只是一个简单的、仅支持入站防护、基于主机的状态防火墙。Windows Server 2008 内置了一个功能强大的高级防火墙。高级防火墙采用了新的图形化界面,对入站、出站信息进行双向过滤,与 IPSec 有更好的配合,更可以配置高级规则。高级防火墙的加入,无疑增加了服务器的安全性,但也增加我们配置服务器的难度,为了降低初学者配置服务器的难度,这里选择关闭服务器防火墙。具体步骤如下。

步骤 1:依次选择"开始"→"控制面板"→"Windows 防火墙",打开如图 8-8 所示的窗口,单击"更改设置"打开如图 8-9 所示"Windows 防火墙设置"窗口。

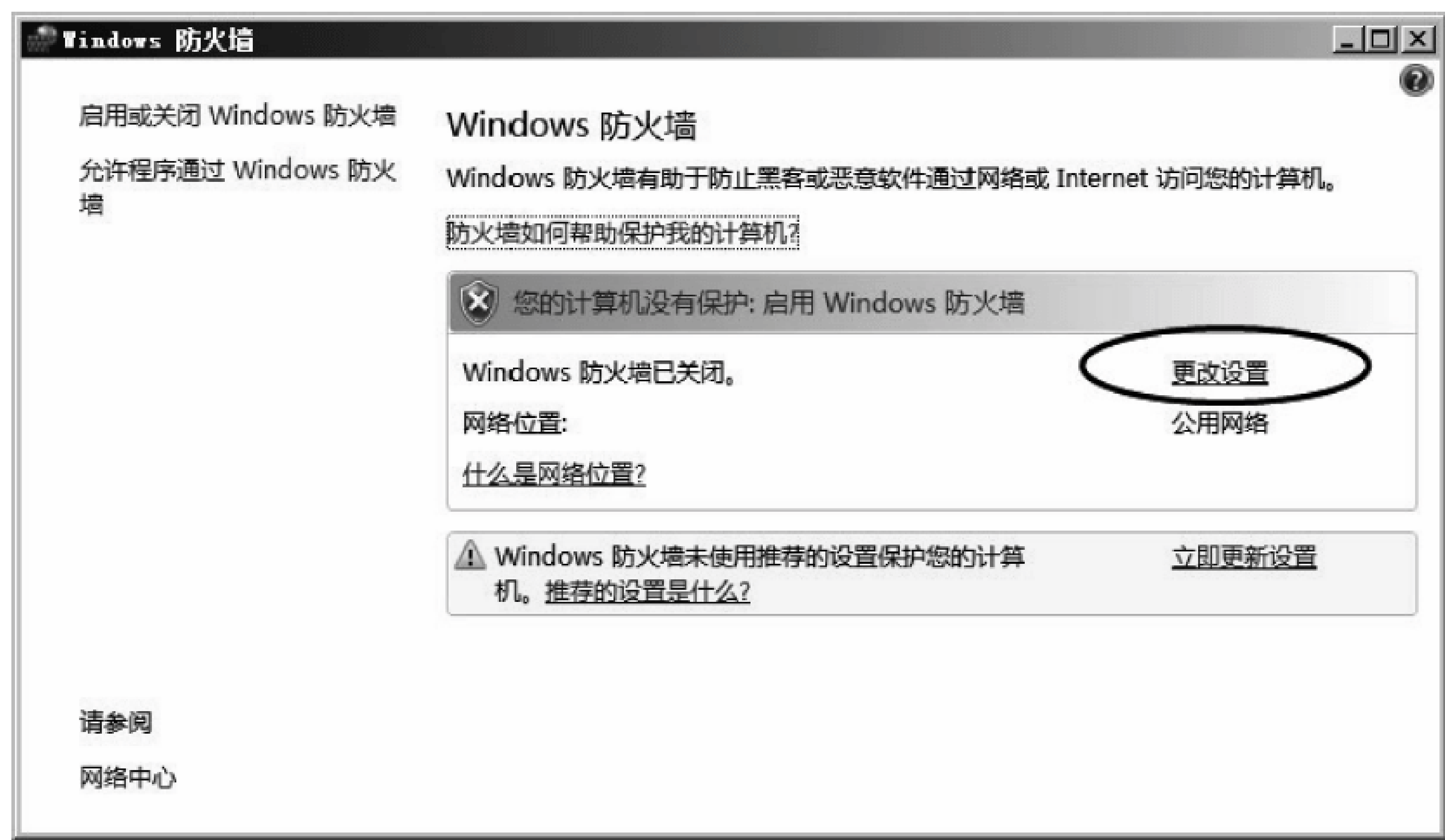



图 8-8 打开防火墙设置窗口

步骤 2：在打开的"Windows 防火墙设置"窗口中，选"常规"选项卡，选择"关闭"单选项，单击"确定"按钮。

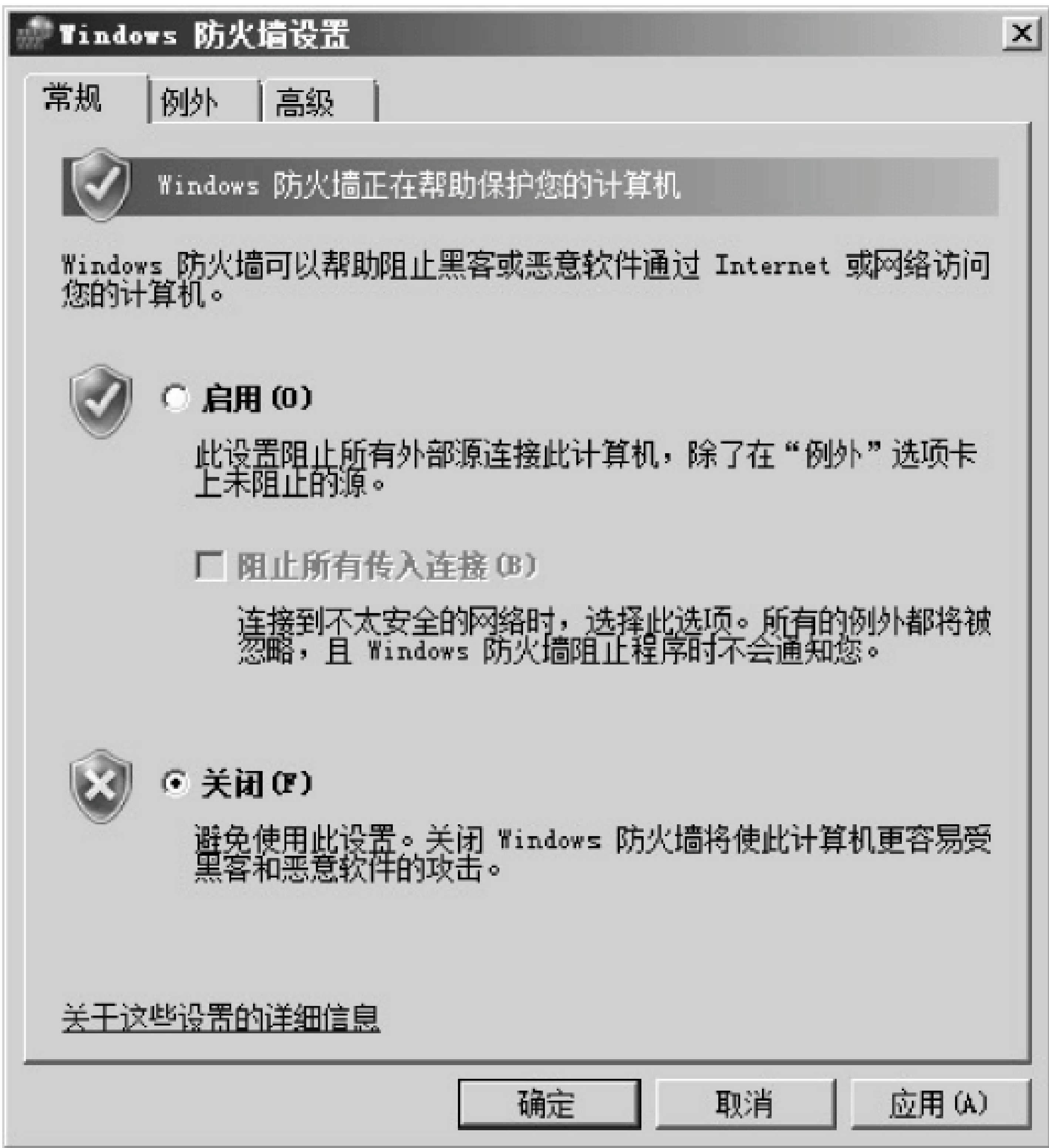



图 8-9　更改 Windows 防火墙设置

# 思考与练习

## 一、填空题

1. 操作系统主要用于________管理、________管理、________管理、________管理和________管理。

2. 网络操作系统的功能主要有________、________、________和________。

3. UNIX 操作系统由________实验室研制的一种________用户________任务的网络操作系统。

4. UNIX 的商业版本主要有 IBM 公司的________、Sun 公司的________、HP 公司的________、微软公司的________、硅谷图形公司(SGI)的________等。

5. Linux 是由芬兰的叫________的学生开发的一种开源的操作系统。

6. 目前 Linux 比较有名的发行版本有________、________、________、________。

## 二、选择题

1. 以下（　　）不是网络操作系统。

A. DOS　　B. Linux　　C. UNIX　　D. NetWare

2. 以下（　　）是开源操作系统。

A. Windows 2008　　B. Linux　　C. AIX　　D. DOS

3. 以下不属于 Windows 2008 的版本是（　　）。

A. 标准版　　B. 企业版　　C. 数据中心版　　D. 个人版

**三、思考题**

1. 简述 Linux 操作系统的特点。
2. 简述 Windows 2008 的特点。
3. 什么是网络操作系统？简述网络操作系统的工作模式。

第 9 章

# DNS 服务器的配置与管理

## 9.1　DNS　概　述

### 9.1.1　DNS 简介

在 Internet 网络中唯一标识主机的是 IP 地址，每台主机有一个 IP 地址，通过 IP 地址+端口号即可访问 Internet 网络中的资源。IP 地址是一串不好记忆的数字，通过 IP 地址访问网络资源十分困难，人们就将易于记忆的域名和不易记忆的 IP 地址进行映射，用域名去访问网络资源，这样给网络用户带来了方便和快捷。在 Internet 早期，应用程序是通过一个本地文件进行主机名和网络 IP 地址映射的，这种机制在主机不多的小型网络里是可行的，但随着网络规模的扩大，这种机制在网络主机名的唯一性、映射文件的维护以及服务器和网络负载等方面的弊端就暴露出来了。为了解决这个问题 DNS(Domain Name System，DNS)就被设计出来了。

DNS 系统把网络划分为不同的区域，一个区域代表网络中一类资源的集合，并采用一个分布式数据库系统保存着域名和 IP 地址的映射关系，为网络用户提供域名和地址的查询。当用户在浏览器中输入一个要访问的域名时，就会触发一个 IP 地址的查询请求，客户机根据自己的网络配置向 DNS 服务器发出查询域名的请求，DNS 服务器就从数据库中查找这个域名对应的 IP 地址，并将查到的 IP 地址返回给客户机，客户机的浏览器根据这个 IP 地址去访问 Internet 中的特定资源。

### 9.1.2　DNS 的组成

DNS 采用层次化的分布式数据结构，其数据库分布在 Internet 上不同的 DNS 服务器上，每个 DNS 服务器只负责整个域名中的一部分。整个 Internet 网络中的域名采用树形层次化结构，由许多域组成，从上到下依次是根域、顶级域、二级域、三级域等，如图 9-1 所示。

**1. 根域**

最顶层的为根域，位于 DNS 树形结构的顶端，用“.”来表示，全球共有 13 个顶级域服务器，其中一个为主根域名服务器，位于美国；其余 12 个为辅助根域名服务器，9 个位于美国，两个位于欧洲，一个位于亚洲的日本。

互联网名称与数字地址分配机构(The Internet Corporation for Assigned Names and

Numbers，ICANN）是一个非营利的国际组织，它负责世界范围内的 IP 地址的分配，通用顶级域名、国家和地区顶级域名的管理。

根域名服务器中只保存着顶级域名服务器的域名和 IP 地址的对应关系，并不保存其他域名。其他各层的域名服务器也是如此，只保存下层 DNS 服务器或主机的域名与 IP 的对应关系，整个 Internet 域名空间就构成了一个分布式数据库系统，这样有利于 DNS 域名查询时，负载的均衡。

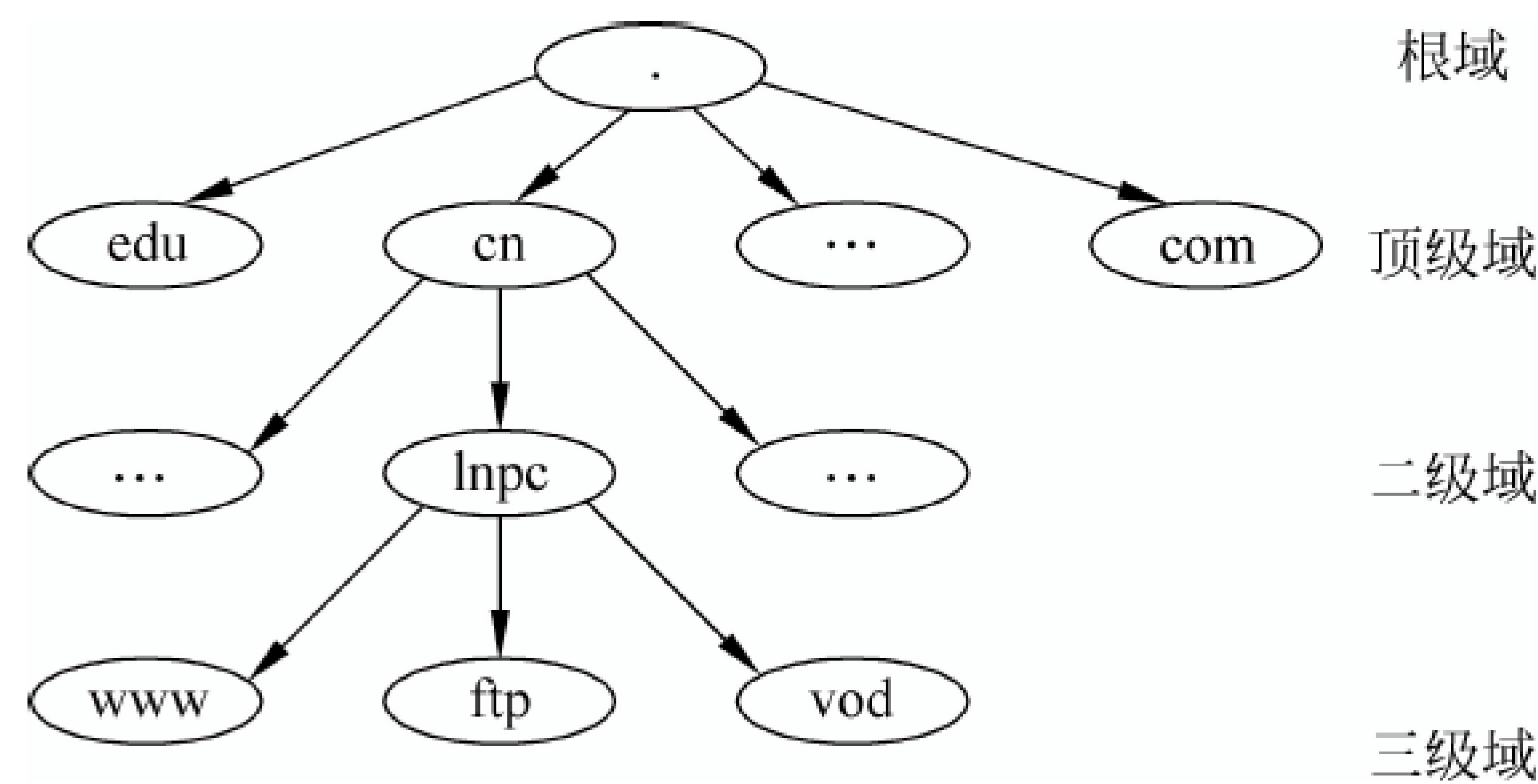



图 9-1　DNS 树形层次结构图

**2. 顶级域**

顶级域是位于根域之下的一层域，顶级域分为两类：一类为机构域名，也称为类别域名，如 www. baidu. com；另一类为地理域名，如 www. lnpc. cn。常用的机构域和地理域见表 9-1。

**表 9-1　常见域名表**

| 机　构　域 | | 地　理　域 | |
|---|---|---|---|
| **域　　名** | **含　　义** | **域　　名** | **含　　义** |
| com | 商业机构 | cn | 中国 |
| edu | 教育机构 | uk | 英国 |
| gov | 政府机构 | de | 德国 |
| int | 国际组织 | fr | 法国 |
| mil | 军事机构 | jp | 日本 |
| net | 网络机构 | hk | 中国香港 |
| org | 非商业机构 | tw | 中国台湾 |
| ac | 科研机构 | mo | 中国澳门 |

ICANN 根据互联网发展需要，在 2000 年 11 月做出决议，从 2001 年开始使用的国际顶级域名也包含另外 7 类：biz、info、name、pro、aero、coop、museum，即第三类顶级域名，也就是所谓的“新顶级域名”。其中前 4 个是非限制性域，后 3 个是限制性域，如 aero 需是航空业公司注册，museum 需是博物馆，coop 需是集体企业（非投资人控制，无须利润最大化）注册。

**3. 子域**

在顶级域之下，都被称为子域，在同一个域中不能有相同的子域。在注册成功的域名之下，可以设置多个子域，如 www. sina. com. cn 中 sina. com 是. cn 的子域。

从 2002 年 12 月份开始，中国互联网络信息中心(China Internet Network Information Center，CNNIC)开放了国内. cn 域名下的二级域名注册，可以在. cn 下直接注册域名，如 www. lnpc. cn。

**4. 主机**

在 DNS 域名空间中，位于最底层的是主机名，如 www. qq. com 中的 www，ftp. lnpc. cn 中的 ftp 都是主机名。在已经注册成功的域中可以根据自己的需要设置主机。

## 9.1.3　DNS 的查询模式

按照 DNS 的查询方式，可以把 DNS 查询方式分为正向查询和反向查询。正向查询是 DNS 查询的主要方式，它根据客户提出的域名，在 DNS 数据库中查询出 IP 地址；反向查询是根据用户提出的 IP 地址查询出其对应的域名。

**1. 正向查询**

在 DNS 查询中，客户执行的大部分都是正向查询。正向查询是基于存储在主机资源记录(A)中记录的主机和 IP 的映射关系，根据域名查询 IP。也就是说，当客户在浏览器中输入一个资源的域名时，借助于该记录将域名解析为 IP 地址，从而完成从域名到 IP 的查询。

**2. 反向查询**

DNS 反向查询是正向查询的反过程，即用户向 DNS 服务器查询已知 IP 对应的域名，反向查询是基于指针资源记录(PTR)，根据用户提出的 IP 地址，解析出 IP 对应的域名。

## 9.1.4　DNS 的查询过程

DNS 的查询有两种方式，一种是递归查询，另一种是迭代查询，下面以查询 www. sina. com. cn 为例进行讲解。

**1. 迭代查询**

(1) 当客户要访问 Internet 上的一个资源 www. sina. com. cn 时，首先向本地的 DNS 服务器提出查询请求，本地的 DNS 服务器会先查询本地的缓存，如果有客户所请求的域名，则返回域名对应的 IP 给客户。

(2) 如果本地 DNS 服务器中没有这个域名，本地域名服务器则代替客户向根服务器(. )发出解析请求，根服务器也没有此记录，但是它知道这个域名的顶级域(. cn)的 DNS 服务器的地址，根服务器把顶级域服务器的地址返回给本地 DNS 服务器。

(3) 本地域名服务器根据根域名服务器返回的地址向. cn 顶级域名服务器发出域名解析请求，. cn 域名服务器也不知道 www. sina. com. cn 的地址，但它知道 com. cn 域名服务器的地址，并把 com. cn 服务器地址返回给本地域名服务器。

(4) 本地域名服务器根据. cn 域名服务器返回的地址，向 com. cn 服务器发出解析请

求，com. cn 域名服务器也不知道 www. sina. com. cn 的地址，但它知道 sina. com. cn 域名服务器的地址，并把 sina. com. cn 服务器地址返回给本地域名服务器。

（5）本地域名服务器向 sina. com. cn 域名服务器发出解析请求，sina. com. cn 域名服务器中包含有 www、mail、ftp 等域名记录。把 www. sina. com. cn 记录的地址返回给本地域名服务器。

（6）本地域名服务器把得到的 www. sina. com. cn 地址返回给客户，客户向 www. sina. com. cn 服务器发出资源访问请求。

这个查询过程是一个迭代的过程，所以我们把它叫做迭代查询，如图 9-2 所示。

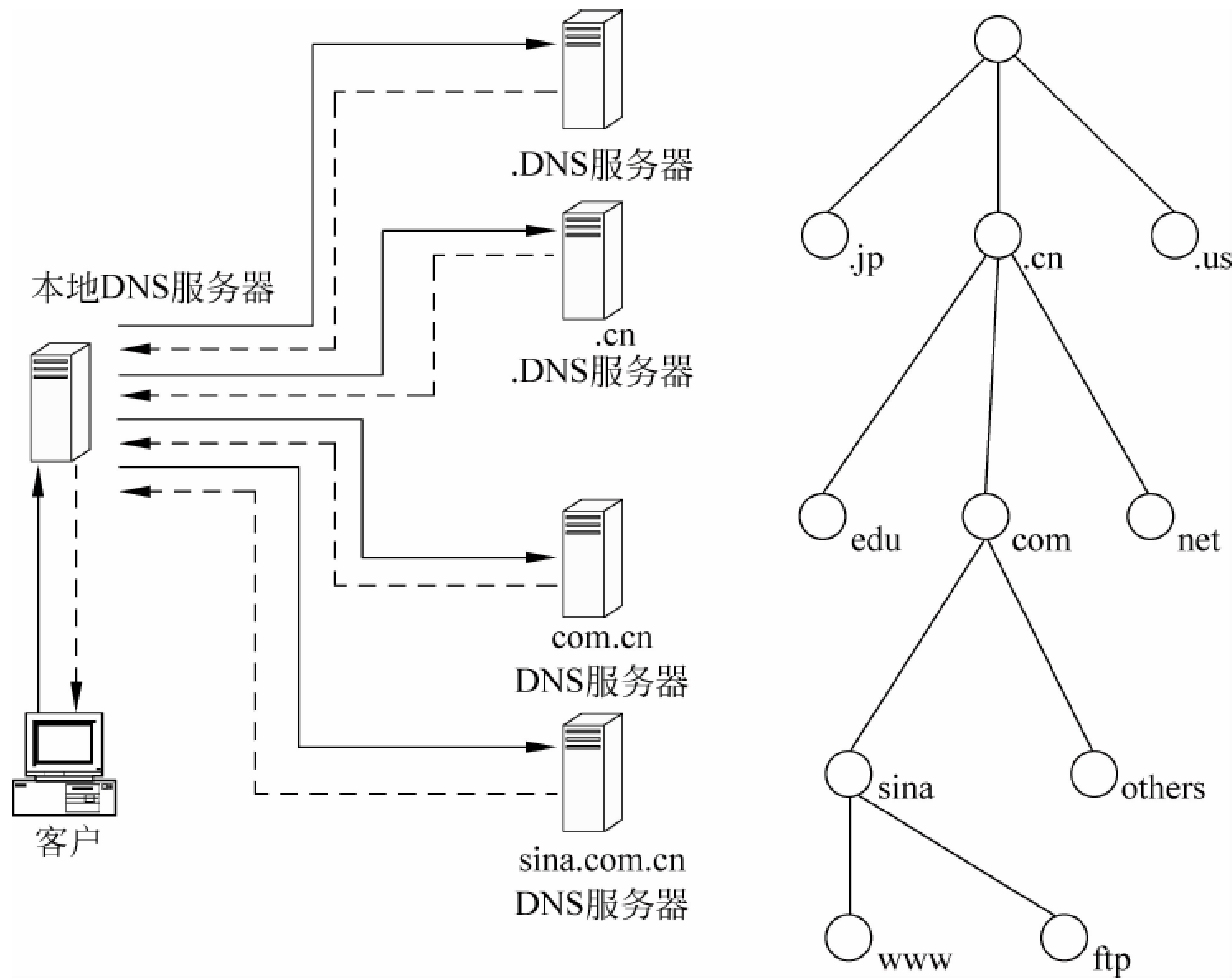



图 9-2　迭代查询示意图

**2. 递归查询**

DNS 客户端从本机配置中获得域名服务器地址，向该域名服务器发出域名解析请求，该域名服务器中没有所要查询的域名，它不向客户端返回查询结果，而是直接向另外的域名服务器 2 转发客户端的请求。域名服务器 2 可能也没有该域名，它也会转发这个解析请求，依此类推，直到查询出正确的地址，或者由最后一个 DNS 服务器告诉客户 DNS 解析错误。最终查询结果会沿着送出解析请求路线反序回送到 DNS 客户端。这个过程是一个递归过程，我们把它叫做递归查询，如图 9-3 所示。

### 9.1.5　网络资源利用过程

网络资源利用过程（图 9-4）如下。

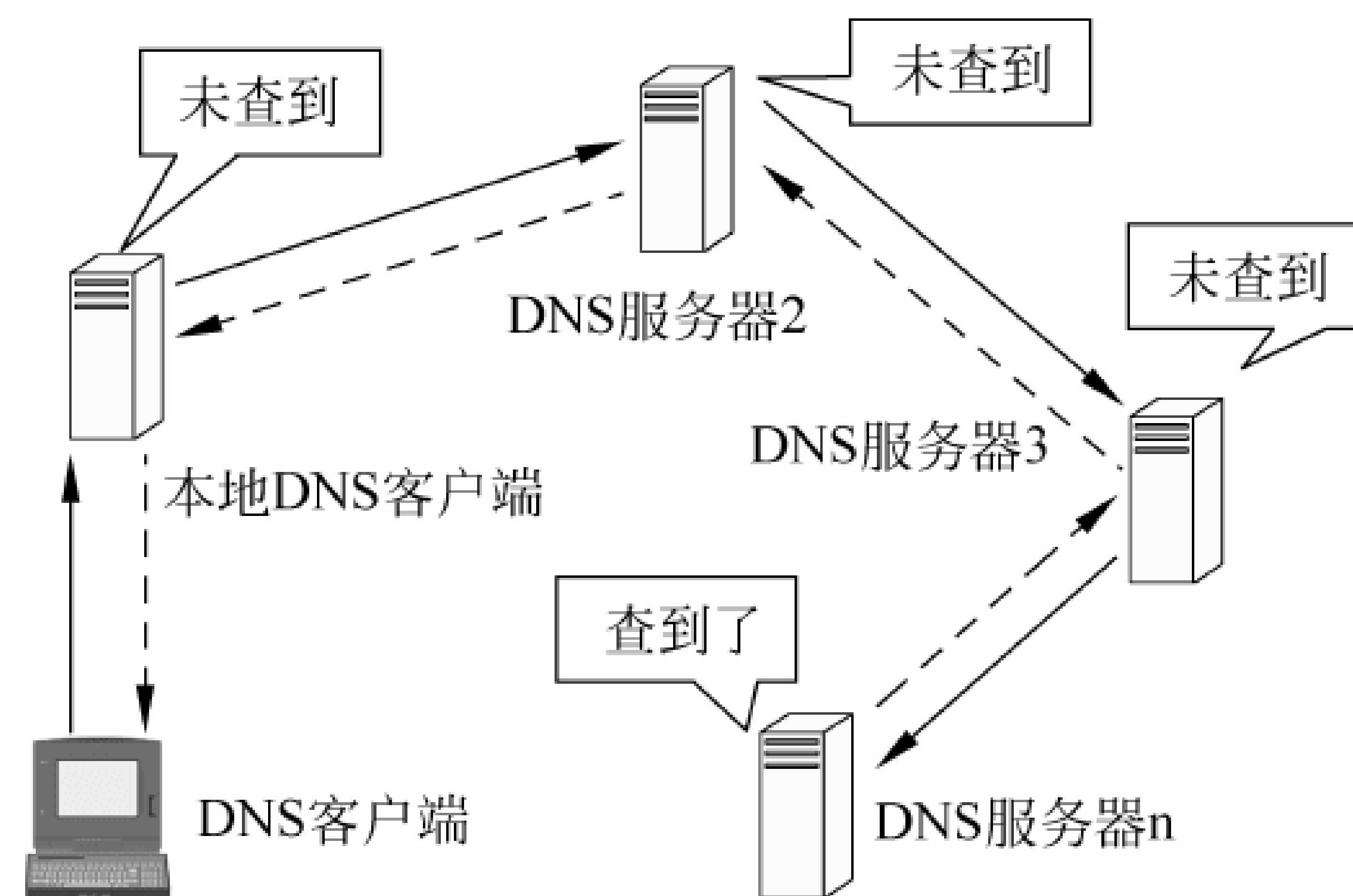



图 9-3　递归方式查询示意图

(1) 客户机要访问 www.sina.com.cn 网络资源。

(2) 客户机向本地 DNS 服务器提出 DNS 解析请求。

(3) 本地 DNS 服务器查询自己的数据库，如果有域名与 IP 的映射关系。则到步骤(7)。如果本地 DNS 服务器的数据库中没有该记录，则检查缓存，如果有该记录则到步骤(7)。

(4) 如果缓存中也没有该记录，则向其他 DNS 服务器发出解析请求。

(5) 其他 DNS 服务器返回 www.sina.com.cn 相匹配的 IP 地址 58.63.236.238。

(6) 本地 DNS 服务器把其他服务器发回的 IP 发送给客户机。

(7) 客户机向地址为 58.63.236.238 的网络服务器请求资源。

(8) 网络服务器把网络资源发送给客户机。

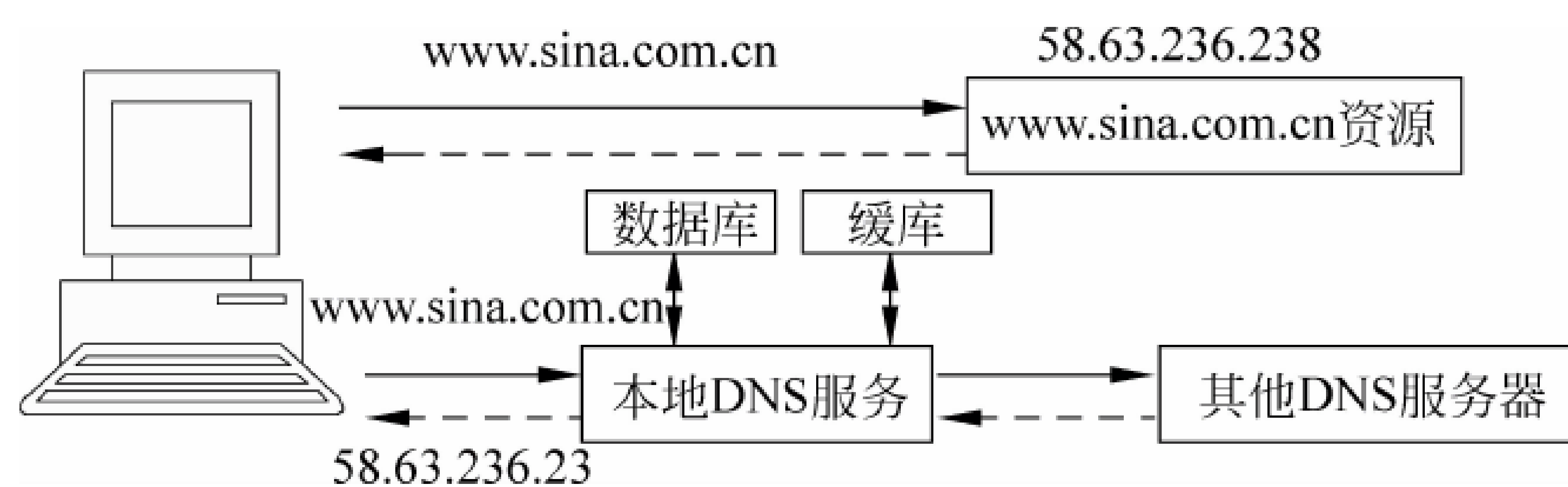



图 9-4　网络资源利用过程

### 9.1.6　DNS 服务器的类型

Internet 中有 4 种类型的域名服务器。

**1. 主域名服务器**

主域名服务器是特定域中所有信息的授权来源，它从管理员创建的本地磁盘文件中加载域信息。该文件包含着服务器具有管理权的 DNS 域的最精确信息。当 DNS 域中的信息发生变化时，这些变化会保存到主域名服务器中的区域文件中。一个域中只能有一个主域名服务器，有时为了分解域名解析的任务，实现域名解析负载的平载，还需要建立一个或多

个辅助域名服务器。

**2. 辅助域名服务器**

辅助域名服务器是主域名服务器的备份,有时又称为备份域名服务器,它具有主域名服务器的绝大部分功能。辅助域名服务器区域文件的内容是从主域名服务器复制过来的,不能更改该区域文件,域信息的更改只在主域名服务器的区域文件中进行。辅助 DNS 服务器主要是用于主域名服务器的负载均衡和容错处理。

**3. 缓存域名服务器**

缓存域名服务器记录着每一个从远程域名服务器传送过来的查询结果,然后保存在缓存中,以备将来对同一信息的查询。缓存域名服务器没有本地数据库,仅起到缓存的作用。缓存域名服务器不能独立存在。

**4. 转发域名服务器**

转发服务器可以将要解析的域名请求发送给网络以外的域名服务器。当转发服务器接到域名解析请求后,它首先查询缓存中是否有该记录的缓存,有则发送给客户端;若没有则把解析请求转发给其他域名服务器。接到域名解析结果后,把解析信息转发给客户端,同时缓存一份,以备将来查询相同记录。

# 9.2 DNS 服务器的安装与配置

## 9.2.1 DNS 服务器的安装

**1. DNS 服务器的安装**

从 Windows Server 2008 的快速启动栏单击“服务器管理器”或从“开始”→“管理工具”→“服务器管理器”,打开“服务器管理器”窗口,如图 9-5 所示。

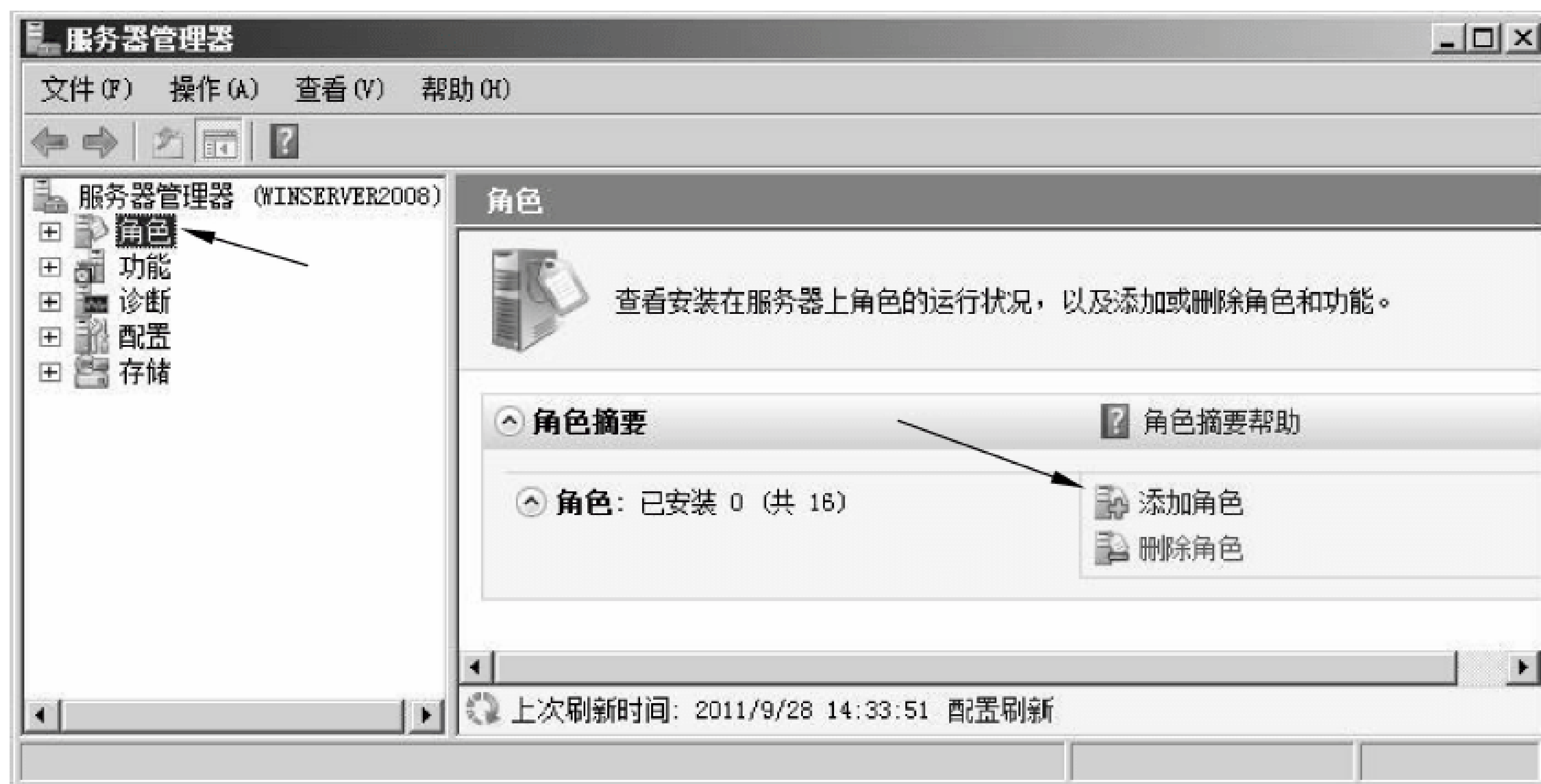



图 9-5 服务器管理器添加角色

单击窗口左边“角色”，窗口右边会显示如图 9-5 所示，单击“添加角色”，打开“添加角色向导”窗口，单击“下一步”，进入到“选择服务器角色”，单击“DNS 服务器”复选框，如图 9-6 所示。




图 9-6　选择 DNS 服务器角色

单击“下一步”，进入到“确认”安装步骤，单击“安装”按钮后，开始安装，经过一段时间的等待，完成安装，单击“关闭”按钮，关闭“安装向导”窗口。

**2. 启动、停止 DNS 服务**

方法一：安装完成以后，在“服务器管理器”窗口中，展开“角色”，单击“DNS 服务器”，会显示如图 9-7 所示的窗口界面。在这里，选择右侧“系统服务”栏目中的 DNS Server，其右侧有“停止”、“启动”、“重新启动”等按钮，通过单击这些按钮即可实现启动/停止 DNS 服务，如图 9-7 所示。

方法二：依次选择菜单“开始”→“管理工具”→DNS，打开“DNS 管理器”，在服务器名上右击，在弹出的菜单中选择“所有任务”→“停止”，即可停止 DNS 服务；选择“所有任务”→“暂停”即可暂停服务；选择“所有任务”→“重新启动”即可重新启动 DNS 服务，如图 9-8 所示。




图 9-7 启动/停止 DNS 服务方法一




图 9-8 启动关闭 DNS 服务方法二

方法三：依次选择“开始”→“管理工具”→“服务”，打开如图 9-9 所示的“服务”窗口，选择 DNS Server 服务，单击工具栏上的“停止”、“暂停”、“重新启动”按钮；或单击窗口中部的“停止此服务”、“暂停此服务”或“重启动此服务”；或右击 DNS Server，选择弹出菜单中的“启动”、“停止”、“暂停”、“重新启动”，即可完成相应的功能。

### 9.2.2 建立正向查找区域

DNS 服务器作为网络中的重要主机，必须要有静态 IP 地址、主机名、域等配置信息，具体配置方法请参见 8.3.3 小节的设置方法。如果服务器不在网络中，则需要连接一条网线，

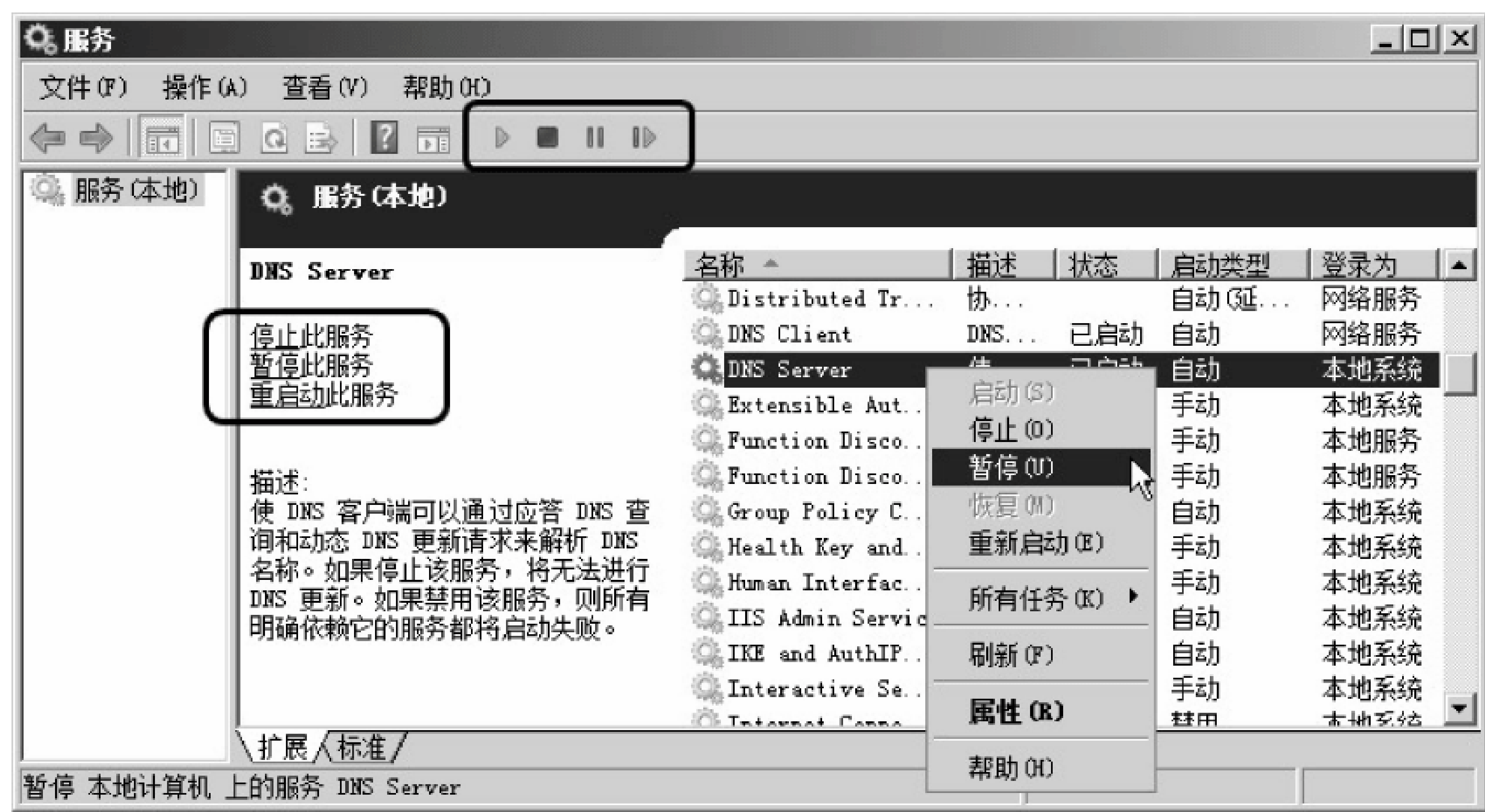



图 9-9　启动关闭 DNS 服务方法三

网线另一端连接一个网络设备(交换机或路由器)。

创建正向查询区域的步骤如下。

步骤 1：依次选择"开始"→"管理工具"→DNS，打开"DNS 管理器"窗口，

步骤 2：右击窗口左侧"正向查找区域"，选择弹出菜单中的"新建区域"，如图 9-10 所示。




图 9-10　新建区域

步骤 3：在出现的"新建区域向导"窗口中选择区域类型，这里选择"主要区域"，如图 9-11 所示。

步骤 4：单击"下一步"，在图 9-12 所示的窗口中设置区域名称。这里设置为 lnpc. cn。

步骤 5：在向导的"区域文件"窗口中，选择"创建新文件，文件名为(c)："选项，创建的正向区域文件为 lnpc. cn. dns。该文件存放在"%SystemRoot%\system32\dns"目录下。

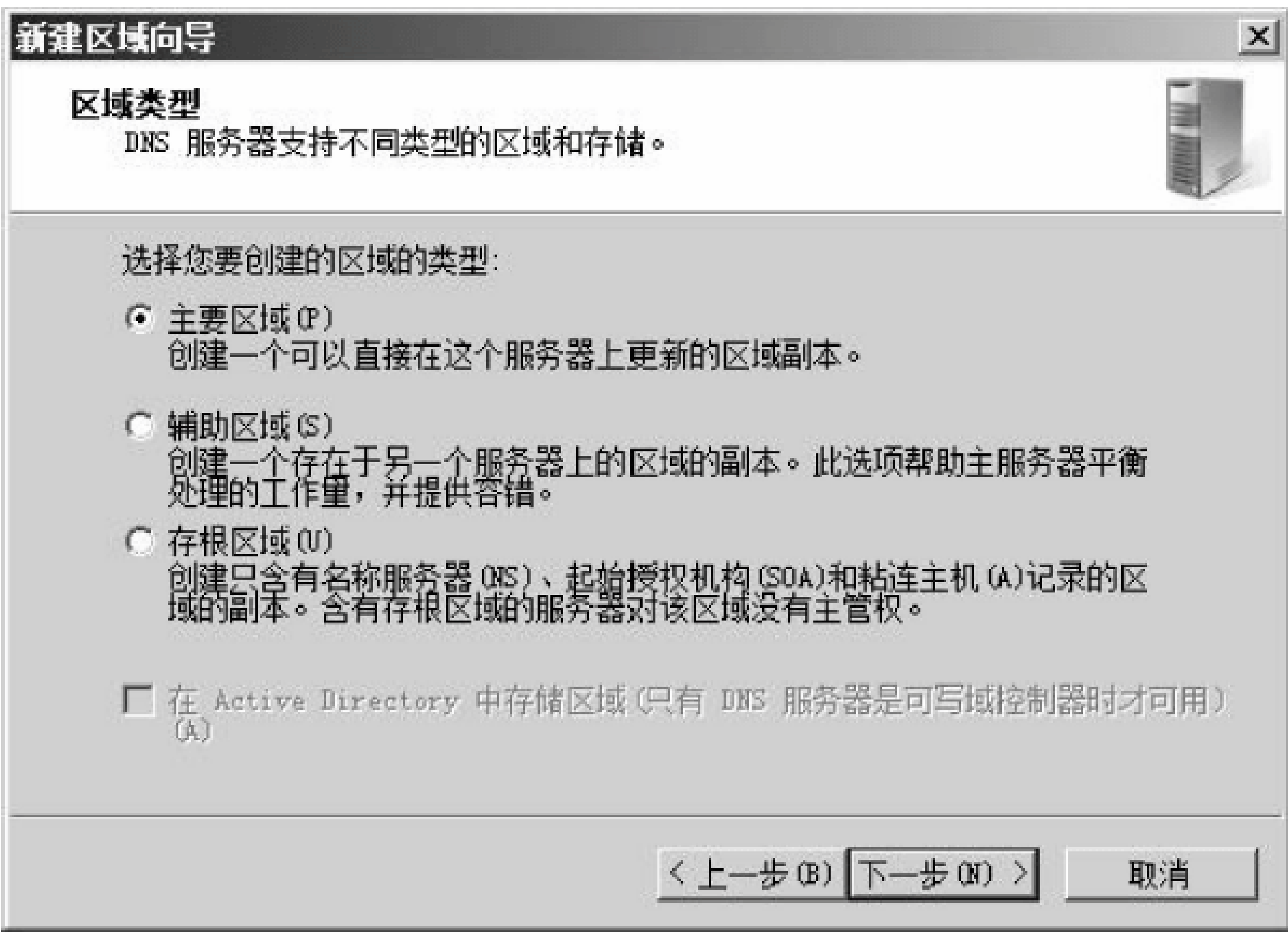



图 9-11 选择区域类型

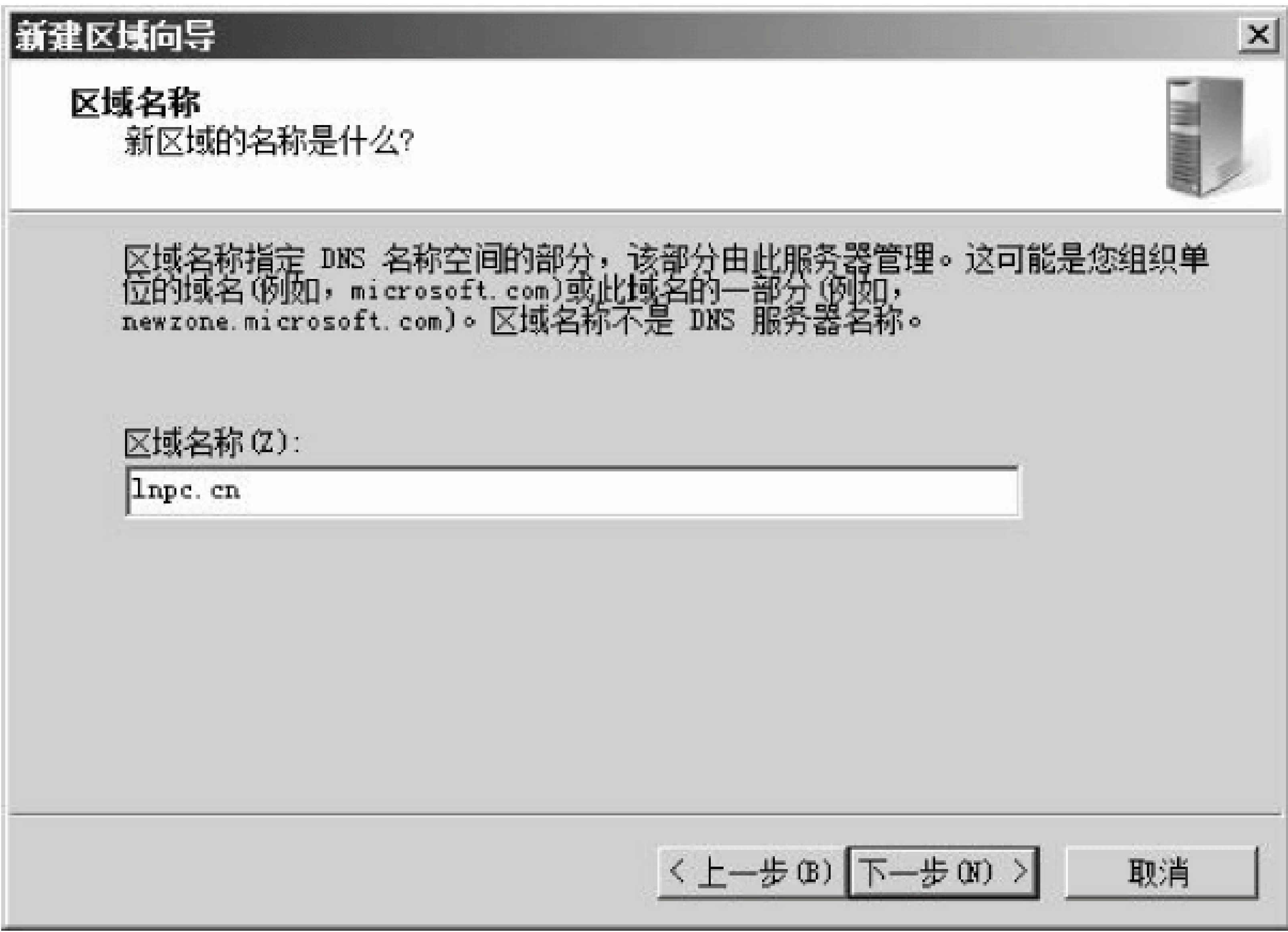



图 9-12 设置区域名称

步骤 6：在向导的“动态更新”窗口中，选择“不允许动态更新”。

步骤 7：在向导的“正在完成新建区域向导”窗口中，单击“完成”。

步骤 8：在“DNS 管理器”窗口左侧，展开“正向查找区域”，即可看到新创建的正向区域 lnpc.cn。

### 9.2.3 新建反向查找区域

创建正向查找区域的目的是为了实现从域名到 IP 的映射，反向查找区域的作用是便于实现从 IP 地址到域名的查找。创建反向查找区域的步骤如下。

步骤 1：执行“开始”→“管理工具”→DNS 命令，打开“DNS 管理”窗口。

步骤 2：展开“DNS 管理”窗口左侧的服务器，单击“反向查找区域”，选择菜单“操作”→“新建区域”；或右击“反向查找区域”，选择弹出菜单中的“新建区域”。

步骤 3：在向导的“区域类型”窗口中，选择“主要区域”。

步骤 4：在向导的“反向查找区域名称”窗口中，选择“IPv4 反向查找区域”，如图 9-13 所示。

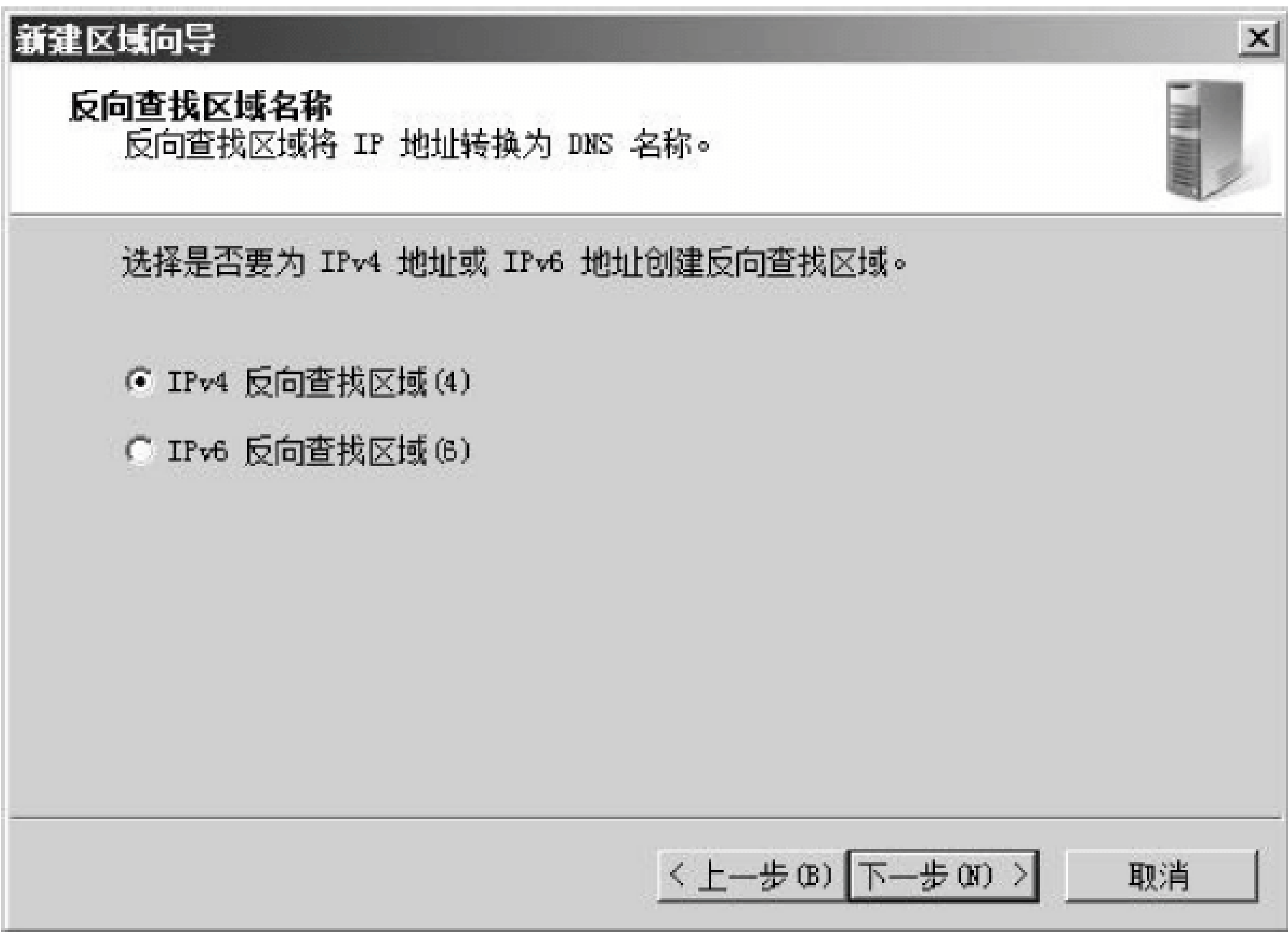



图 9-13　选择反向查找区域名称

步骤 5：在向导的“输入网络 ID 或网络名称”窗口中，输入网络 ID。请注意用正常顺序输入网络 ID，Windows 2008 会自动将网络 ID 顺序反过来，形成反向查找区域名称。如输入的网络 ID 号为 192.168.13，则形成的反向查找区域名称为 13.168.192.in-addr.arpa，如图 9-14 所示。

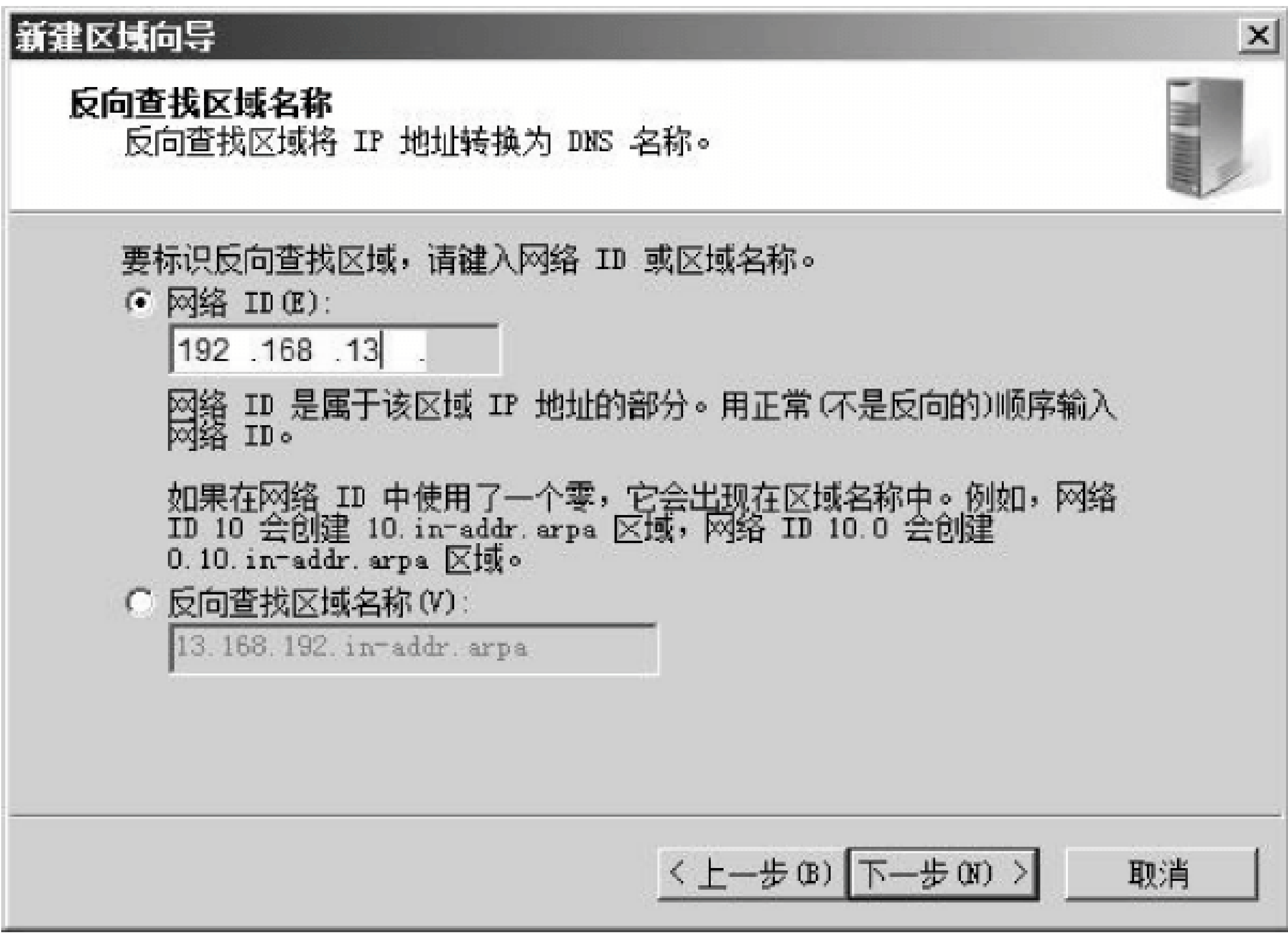



图 9-14　输入网络 ID 或区域名称

步骤 6：创建新反向区域文件。形成 13.168.192.in-addr.arpa.dns，它位于%SystemRoot%\system32\dns 目录下。

步骤 7：在“动态更新”窗口中选择“不允许动态更新”。

步骤 8：在向导的“正在完成新建区域向导”窗口中，单击“完成”。

步骤 9：在“DNS 管理器”窗口左侧，展开“反向查找区域”，即可看到新创建的反向查找区域 13.168.192.in-addr.arpa。

## 9.2.4 建立和管理 DNS 资源记录

### 1. 资源记录类型

DNS 服务器中包括一个或多个区域数据库文件，每个区域数据库文件都有一组结构化的资源记录，资源记录包括 SOA、NS、MX、A、CNAMA 等资源记录类型，当收到客户的名称解析请求后，DNS 服务器会在区域数据库文件中查找资源记录，并给予响应。

9.2.2 节和 9.2.3 节创建区域文件后，在 C:\Windows\System32\dns 目录下创建正向区域文件 lnpc.cn，及反向区域文件 13.168.192.in-addr.arpa，下面以这两个文件为例，介绍资源文件的类型。

lnpc.cn 区域文件大概内容：

```
@                    IN   SOA winserver2008. hostmaster. (
                          3              ; serial number
                          900            ; refresh
                          600            ; retry
                          86400          ; expire
                          3600         ) ; default TTL
@                    NSwinserver2008.
web                  CNAME      www.lnpc.cn.
www                   A          192.168.13.1
```

13.168.192.in-addr.arpa 文件大概内容：

```
@                    IN   SOA winserver2008. hostmaster. (
                          2              ; serial number
                          900            ; refresh
                          600            ; retry
                          86400          ; expire
                          3600         ) ; default TTL
@                    NS   winserver2008.
1                    PTR   www.lnpc.cn.
```

从以上两例可以看出资源文件可以分为以下几类。

1）SOA 记录

区域数据库文件通常以被称为“授权记录开始(Start of Authority, SOA)”的资源记录

开始，此记录用来表示某区域授权服务器的相关参数，其基本格式如下。

```
域名  IN  SOA  DNS主机名  管理员电子邮件地址(
                          序列号
                          刷新时间
                          重试时间
                          过期时间
                          最小生存期)
```

SOA 记录首先需要指定区域名称，通常用“@”表示域名，由于“@”符号在区域文件中的特殊含义，管理员的电子邮件地址中不能使用“@”，而使用“.”符号代替。

IN 代表 Internet 类，SOA 是起始授权类型。

序列号也称为版本号，用来表示该区域数据库的版本大小，它可以是任何数字，只要它随着区域中记录修改不断增加即可，即新版本号应比旧版本号要大。

刷新时间：指定辅助 DNS 服务器根据主 DNS 服务器更新区域数据库文件的时间间隔。

重试时间：指定辅助 DNS 服务器如果更新区域文件时出现通信错误，多长时后重试。

过期时间：指定辅助 DNS 服务器无法更新区域文件时，多长时间后所有资源记录无效。

最小生存时间：指定资源记录信息存放在缓存中的时间。

2）NS 记录

NS 记录用来指明该区域中 DNS 服务器的主机名或 IP 地址，是区域数据库文件中不可缺少的资源记录。如果有一个以上的 DNS 服务器，可以在 NS 记录中将它们一一列出，这些记录通常放在 SOA 记录后面。

3）MX 记录

MX 记录仅用于正向区域文件，它用来指定本区域的邮件服务器主机名。

4）A 记录

A 记录指明区域内的主机域名与 IP 地址的对应关系，仅用于正向区域文件。

5）AAAA 资源记录

将 DNS 域名映射到 IPv6 的 128 位地址中。

6）CNAME 记录

CNAME 记录用于为区域中的主机建立别名，仅用于正向区域文件。别名通常用于一个 IP 地址对应多个不同类型服务器的情况。如 lnpc.cn 区域文件中有

```
web          CNAME      www.lnpc.cn.
```

该资源记录表明 web.lnpc.cn 域名是 www.lnpc.cn 的别名。

7）PTR(Point)

该资源记录与主机记录配对，可将 IP 地址映射为 DNS 反向区域中的主机名。如

13.168.192.in-addr.arpa 文件中有

1　　　PTR　　　www.lnpc.cn.

表示 IP 地址 192.168.13.1 对应的域名为 www.lnpc.cn。

总之，正向区域数据库文件都是由 SOA 记录开始，可以包括 NS 记录、A 记录、MX 记录、CNAME 记录等。

**2. 建立 IPv4 主机记录**

步骤 1：依次选择"开始"→"管理工具"→DNS，打开"DNS 管理器"。

步骤 2：在"DNS 管理器"窗口左侧"正向查找区域"下找到刚才新建的 lnpc.cn 区域，右击，选择弹出菜单"新建主机(A 或 AAAA)"，如图 9-15 所示。

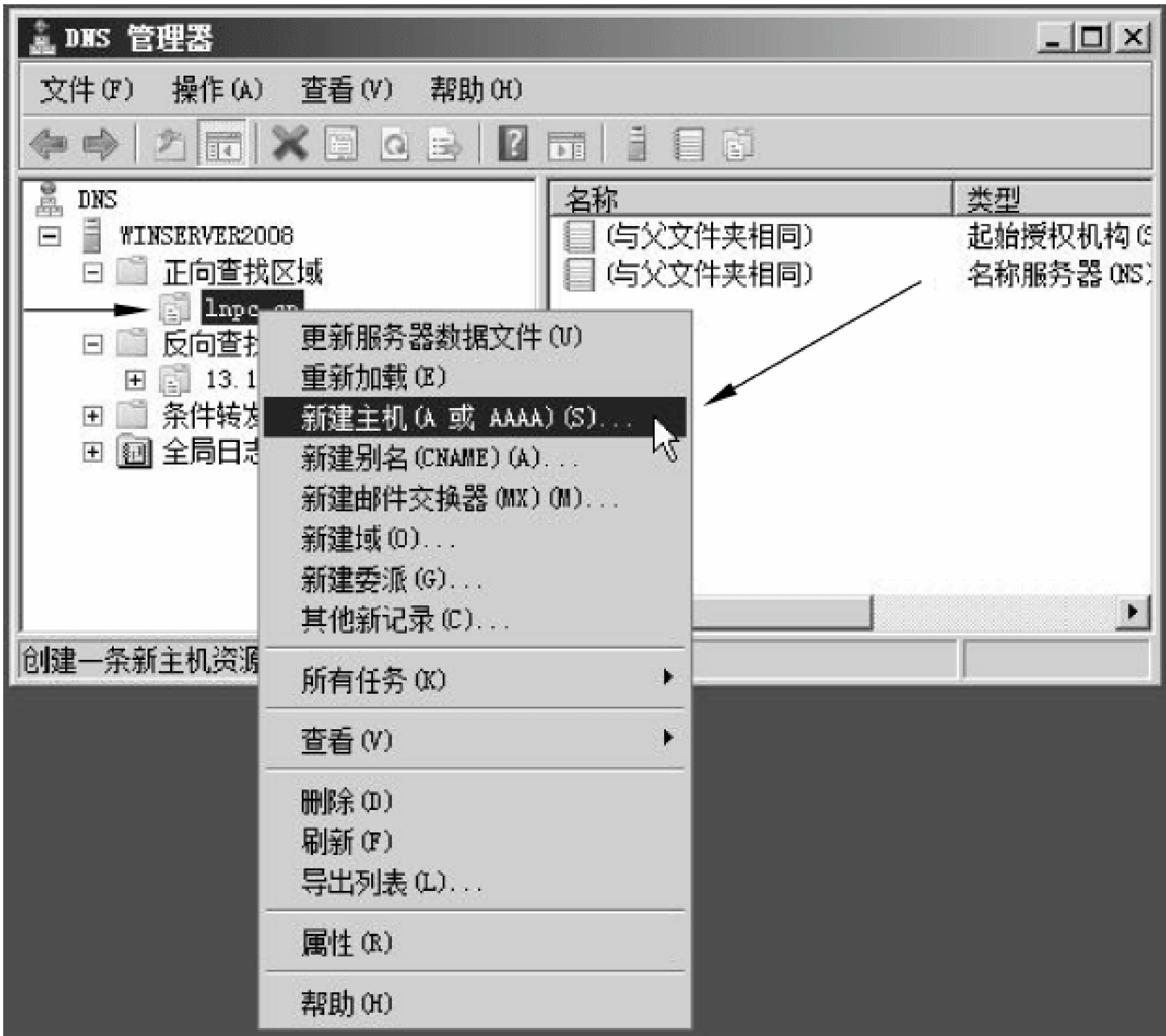



图 9-15　新建主机 A 记录

步骤 3：在打开的新建主机窗口中，输入记录的名称，如本例为 www，系统自动给出域名 www.lnpc.cn；输入域名对应的 IP 地址 192.168.13.1；选中"创建相关的指针(PTR)记录"，则在反向域文件中添加相关的指针(PTR)记录，以实现反向查找，如图 9-16 所示。也可不选中此复选框，仿照建立正向主机记录的方法，建立反向指针记录。这里就不再介绍了。

步骤 4：在"成功创建了主机记录"窗口中单击"确定"按钮。

**3. 给主机名创建别名**

步骤 1：在"DNS 管理器"中右击 lnpc.cn 域，在弹出菜单中选择"新建别名(CNAME)"选项，如图 9-17 所示。

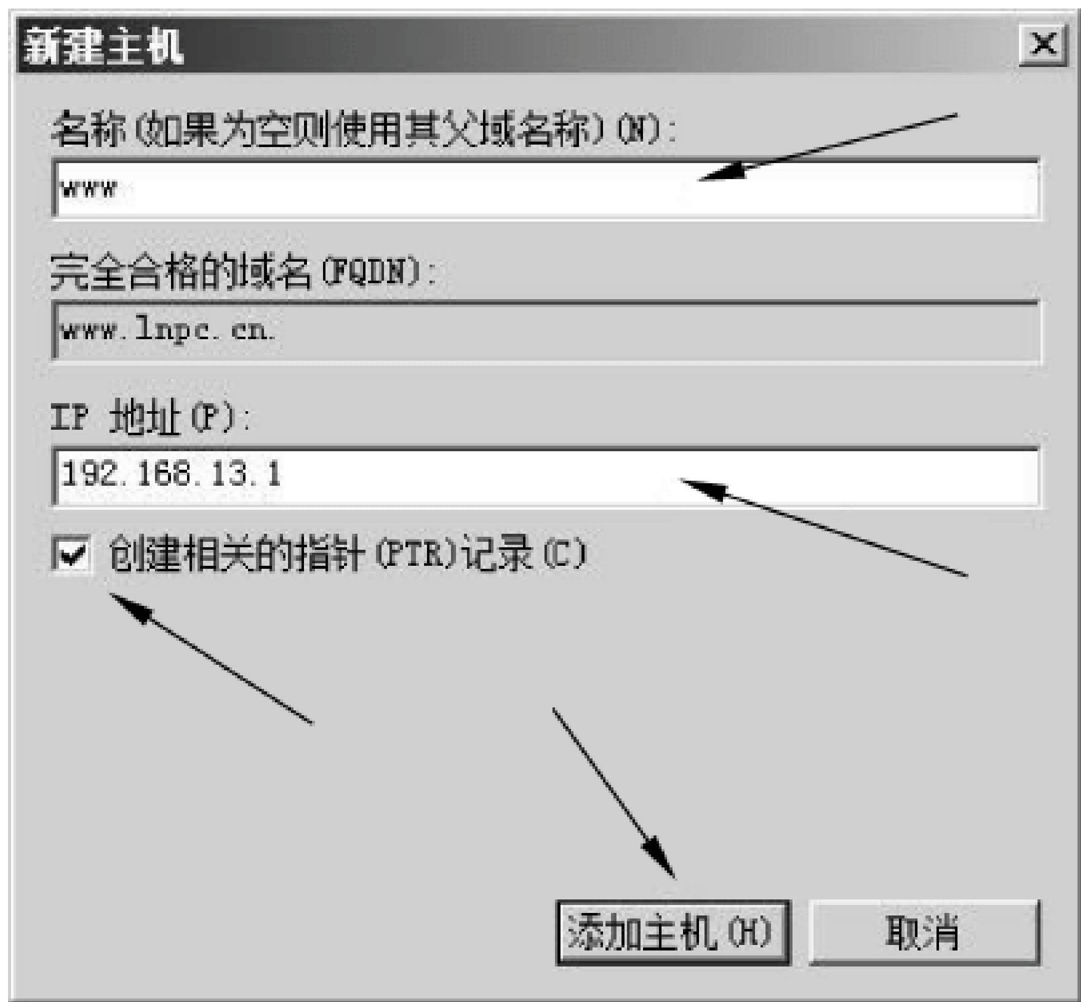



图 9-16　设置主机相关参数

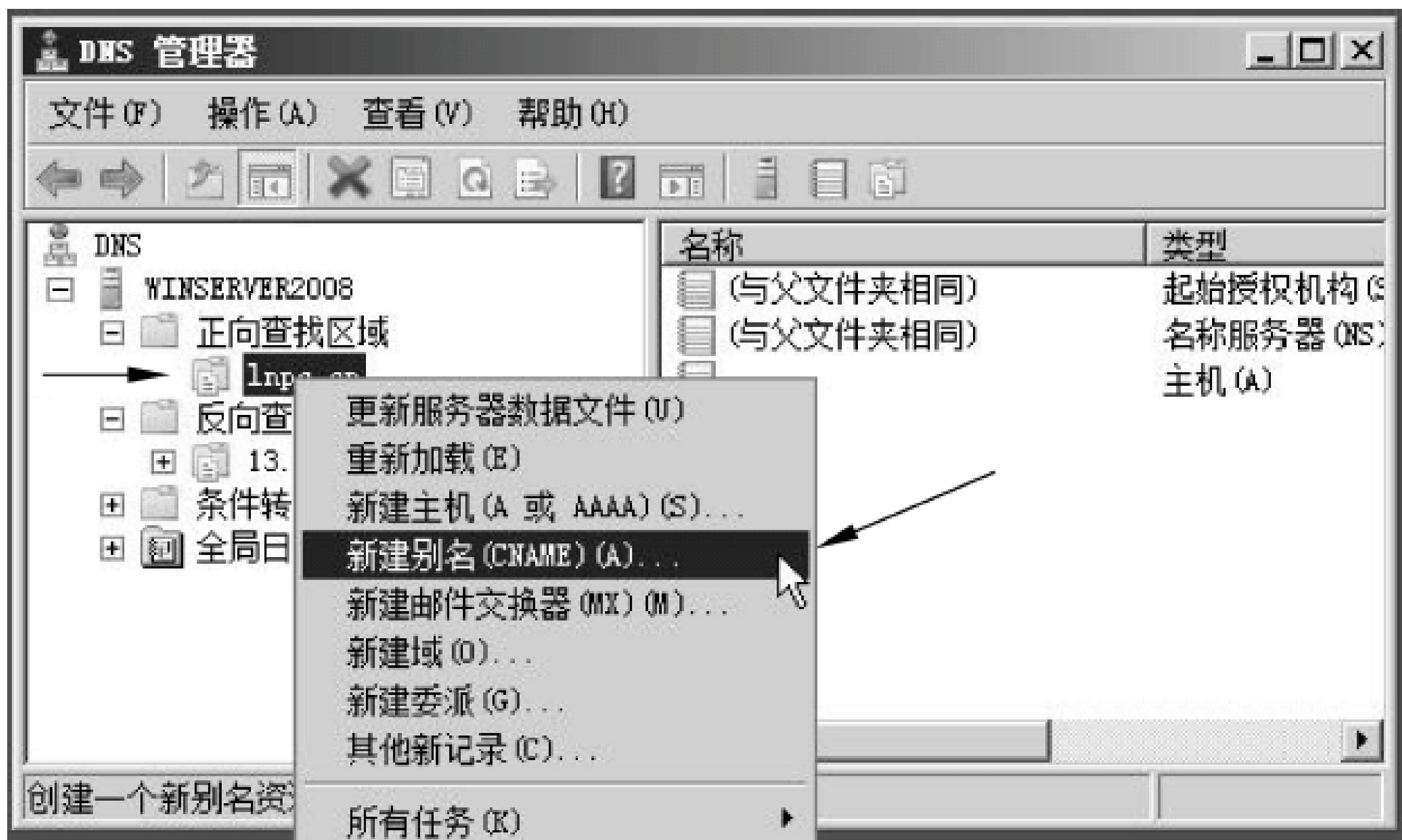



图 9-17　新建别名

步骤 2：在“新建资源记录”窗口中，输入别名 web；在“目标主机的完全合格的域名(FQDN)”中输入域名，或者单击“浏览”按钮，在打开的“浏览”窗口中，从“浏览”下拉列表框中依次双击 DNS→“服务器主机名”→“区域文件名”，在记录列表框中选择 www 项，单击“确定”按钮，完成选择，如图 9-18 所示。

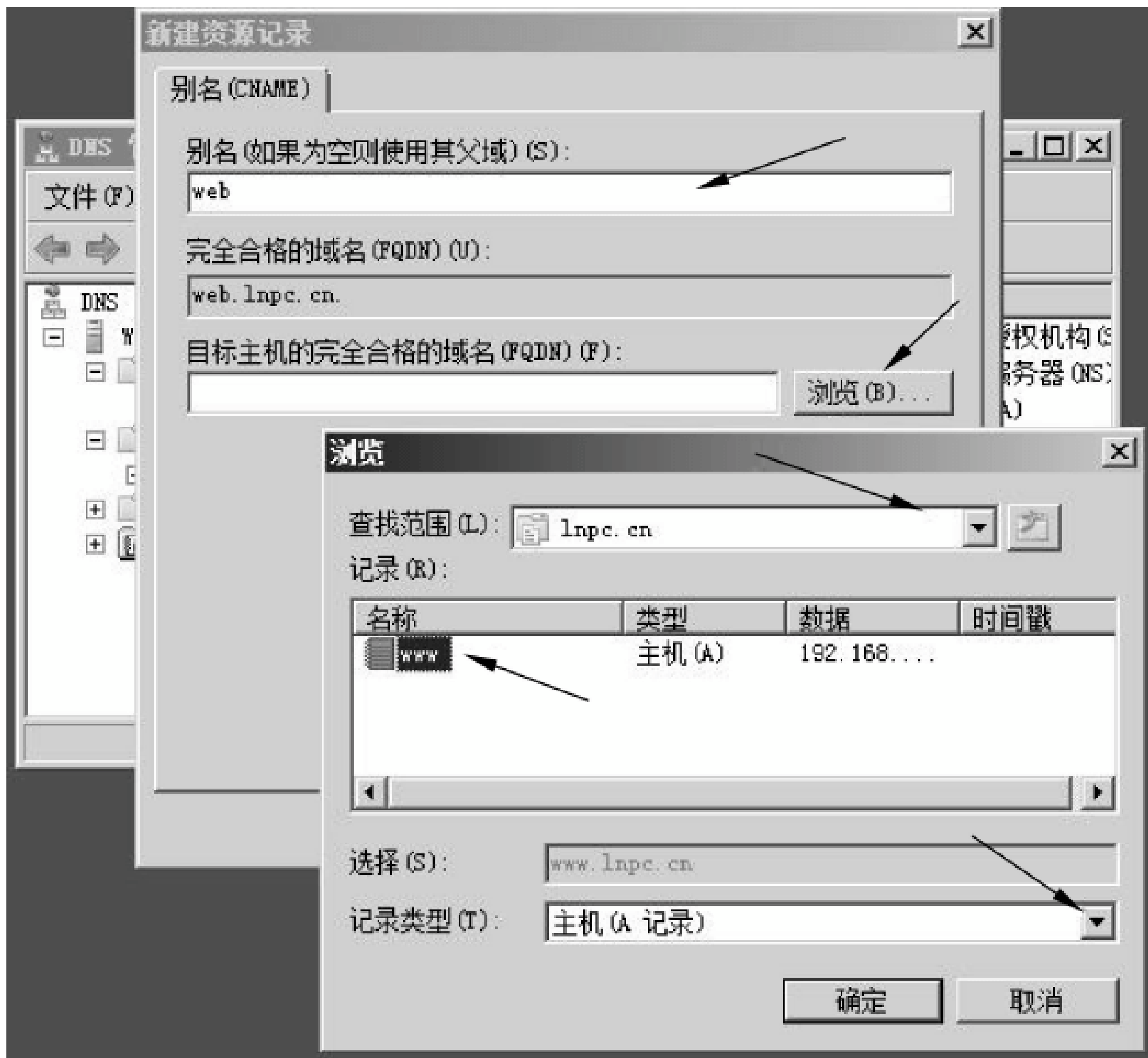



图 9-18　输入别名参数

步骤 3：单击“新建资源记录”窗口中“确定”按钮。

步骤 4：创建完成后的效果如图 9-19 所示，这时，web.lnpc.cn 是 www.lnpc.cn 的别名，网络资源 www.lnpc.cn 和 web.lnpc.cn 是同一资源。




图 9-19　别名效果

## 9.3　DNS 客户机的设置与域名解析

### 1. DNS 客户端设置

DNS 客户端的设置比较简单，本例 DNS 服务器的 IP 地址为 192.168.13.200，则客户端的设置如下所示。

如在 Windows XP 客户端，打开"控制面板"→"网络连接"→"本地连接属性"→"Internet 协议属性"。这个窗口中，设置 DNS 服务器的地址为 192.168.13.200，即 DNS 服务器的 IP 地址，如图 9-20 所示。

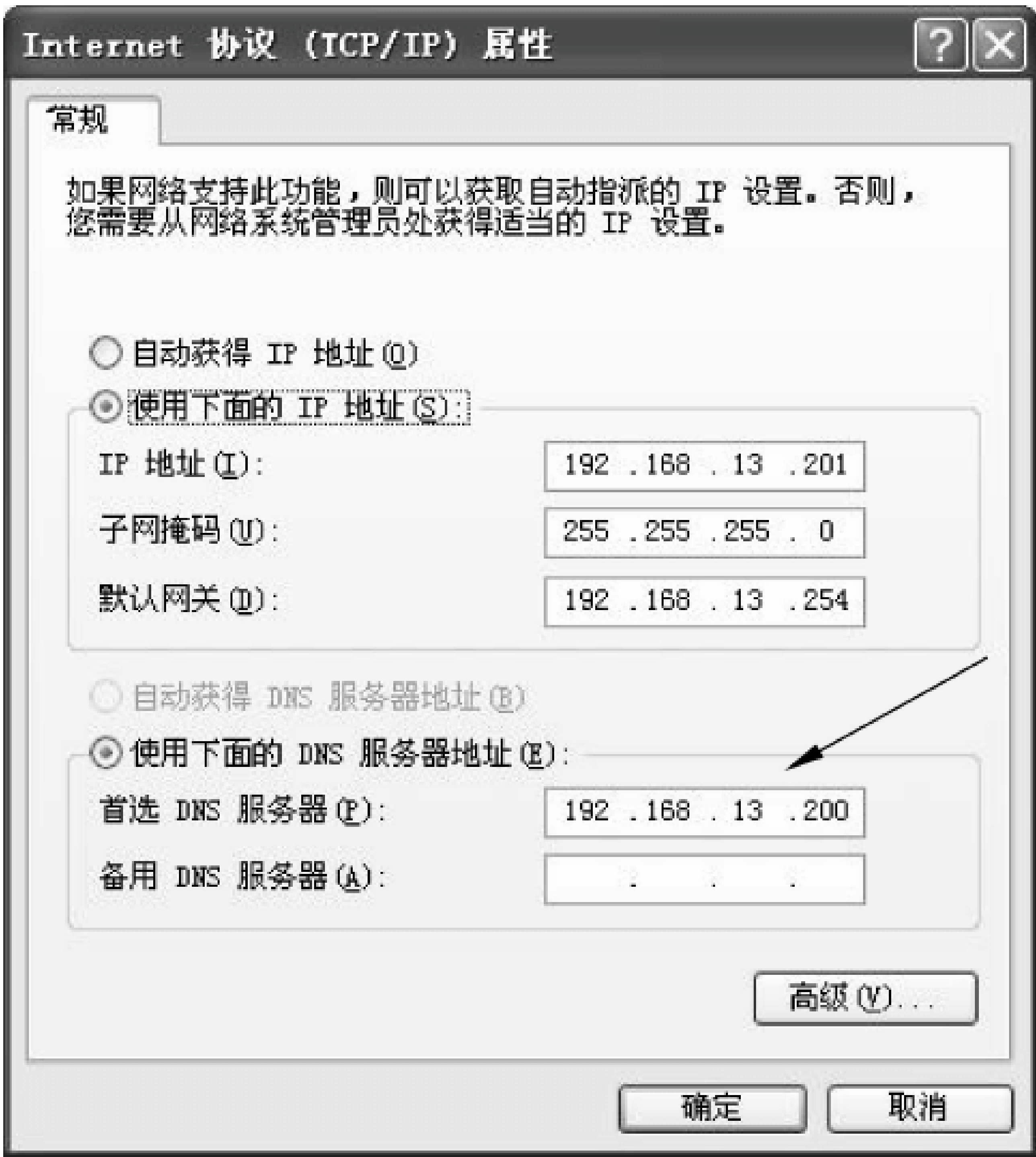



图 9-20　客户端 DNS 服务器地址的设置

**2. DNS 域名的解析**

在客户端，依次选择“开始”→“运行”，输入 cmd，打开“命令提示符”窗口，在窗口中输入 nslookup www.lnpc.cn。

然后，输入 nslookup web.lnpc.cn，查看这两个域名对应的 IP 地址为同一个 IP 地址 192.168.13.1。

也可以在命令行下，输入 ping www.lnpc.cn，可以看出目标主机的网络是连通的。

进行反向查找，输入 nslookup 192.168.13.1，查找到 192.168.13.1 这个 IP 对应的域名为 www.lnpc.cn，如图 9-21 所示。

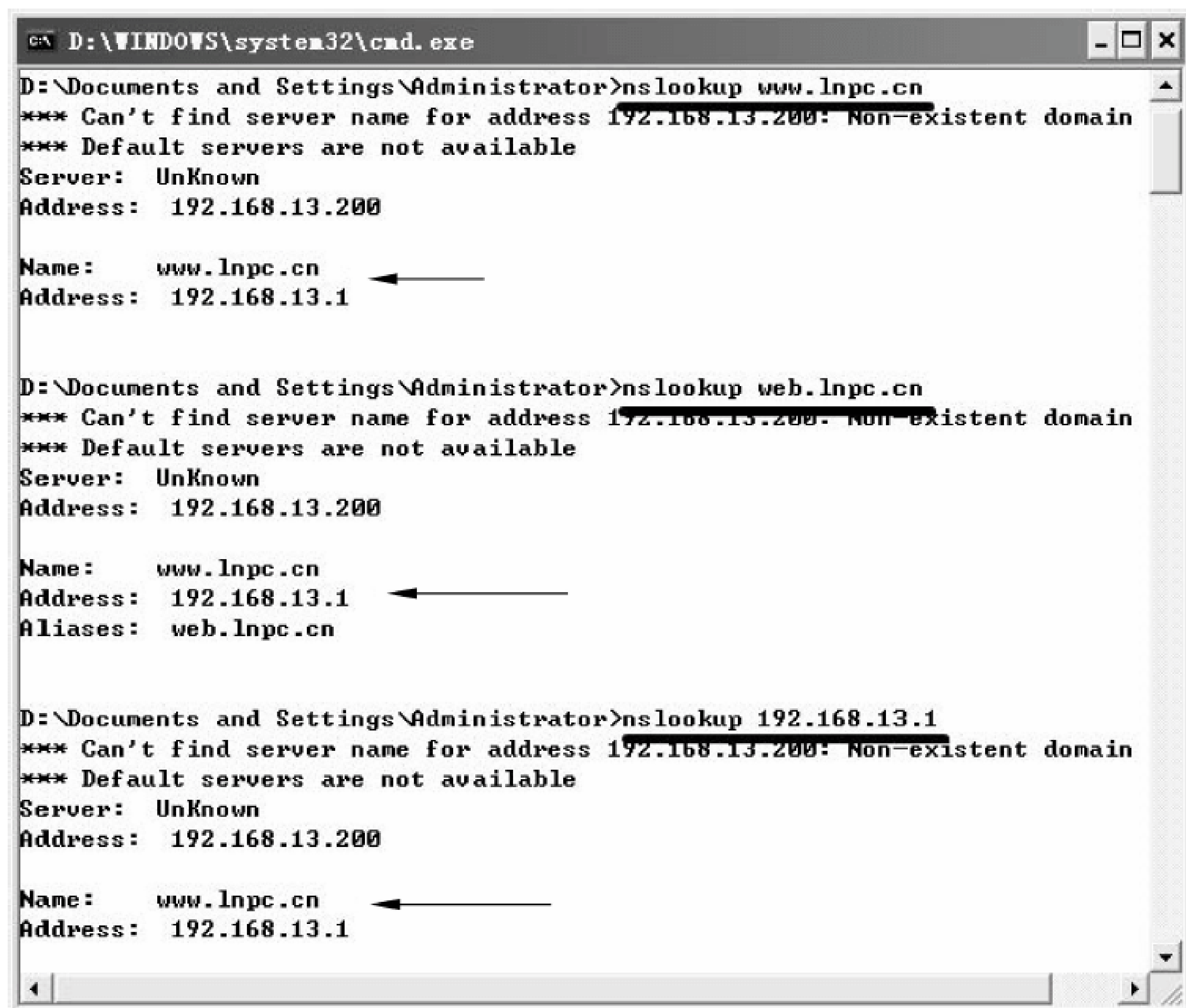



图 9-21　域名的解析

## 9.4　配置 DNS 条件转发器

本地的 DNS 服务器并不能解析所有的域名解析请求，这时本地 DNS 服务器可以把解析请求转发给其他服务器，这被叫做条件转发。下面介绍条件转发器的设置。

在“DNS 管理器”窗口中，右击左侧“条件转发器”，在弹出菜单中选择“新建条件转发器”，如图 9-22 所示。

在“新建条件转发器”窗口的 DNS 域文本框中，输入 DNS 域名 lnjg.edu.cn，在“主服务器的 IP 地址”中输入条件转发器 IP 地址 192.168.13.100。DNS 转发器会自动进行验证，

如图 9-23 所示。




图 9-22 新建条件转发器

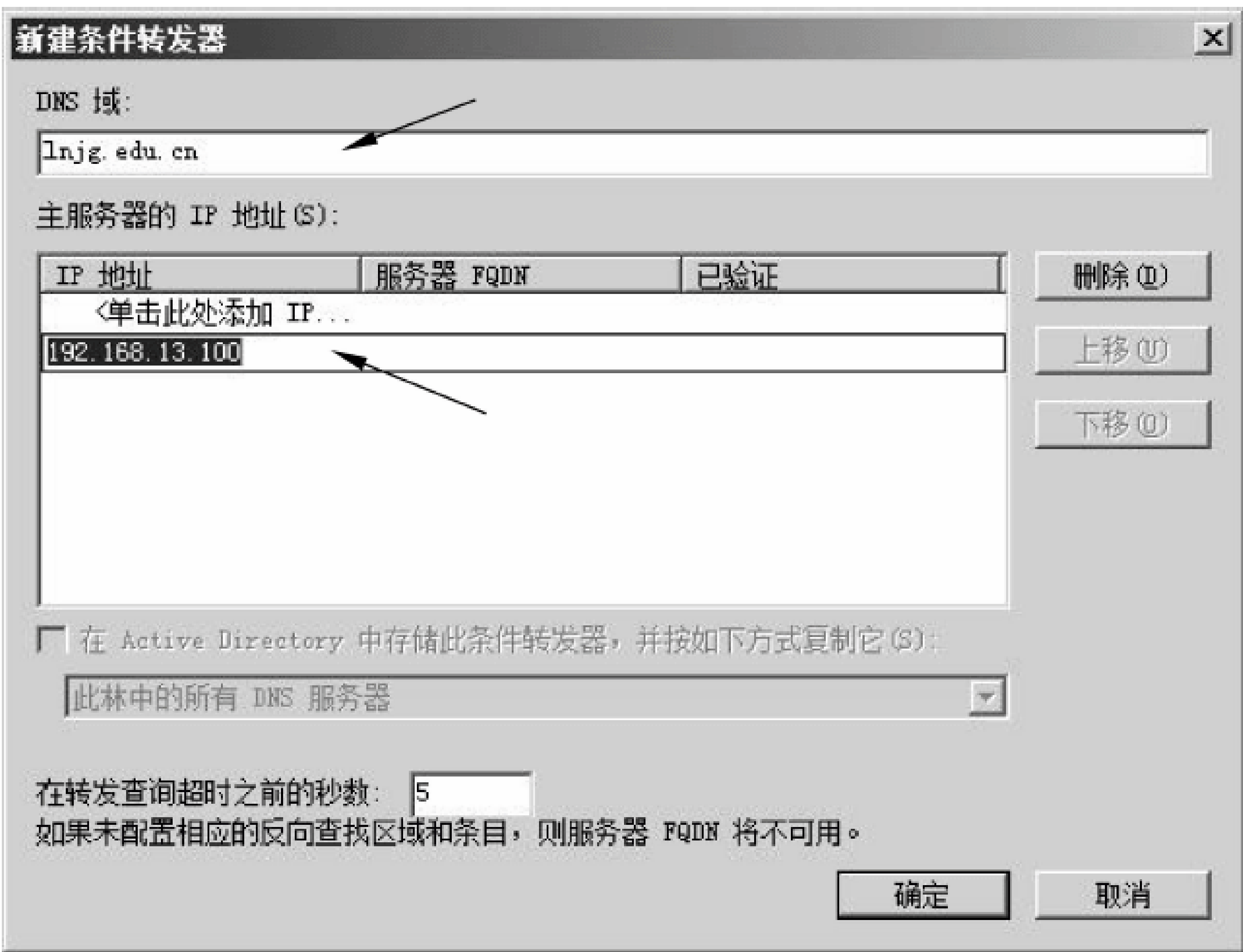



图 9-23 输入条件转发器参数

客户端提出本地域名服务器解析不了的域名解析请求时，条件转发器会按照域名转发给特定的 DNS 服务器，而不是全部转发到一个特定的 DNS 服务器。这样有利于提高 DNS 转发的效率。在配置条件转发器时，首先为其指定转发请求的域名，然后为这个域名指定一个或多个 DNS 服务器。当客户端对配置了条件转发器的 DNS 服务器提出解析请求时，该服务器会首先在自己的数据库和高速缓存中查找，若未找到，配置了指定域名条件转发器的 DNS 服务器会把解析请求转发给那个特定的 DNS 服务器进行解析。

如本地 DNS 服务器中并未配置 www.lnjg.edu.cn 域名，但因为该服务器配置了条件转发服务器，可以把对 lnjg.edu.cn 的解析请求转发给 IP 为 192.168.13.100 的 DNS 服务器解析。

## 9.5 建立辅助 DNS 服务器

主 DNS 服务器是某一特定区域中所有信息的授权来源，这是实现域间通信所必需的。为了防止主 DNS 服务器由于软硬件故障导致的停止 DNS 服务，这就需要在同一网络中部署两台以上的 DNS 服务器，一台作为主 DNS 服务器，另外的机器作为辅助 DNS 服务器。主 DNS 服务器保存的是网络区域信息的主体，可以在主 DNS 服务器上修改区域数据库的内容。而辅助 DNS 服务器保存的信息是区域信息的辅助版本，它只能提供域名查找而不能在辅助 DNS 服务器上修改区域信息。

辅助 DNS 服务器主要有两大作用：一是作为主 DNS 服务器的备份；二是为主 DNS 服务器分担负载。当主 DNS 服务器正常运行时，辅助 DNS 只是起到备份作用；当主 DNS 服

务器出现故障时，辅助 DNS 服务器立即承担起域名解析的重任。

辅助 DNS 服务器从其他 DNS 服务器复制数据的过程叫做区域传输。在下面三种情况下启动区域传输：一是辅助 DNS 服务器刚启动时；二是 SOA 记录中的刷新间隔到达时；三是主 DNS 设置了主动通知辅助 DNS 数据有变化时。上面三种情况之一发生时，辅助 DNS 服务器会主动与主 DNS 服务器进行区域传输。

辅助 DNS 服务器的配置相对较为简单，因为它的区域数据是从主 DNS 服务器传输过来的，无需手工配置。为了安全起见，主 DNS 服务器与辅助 DNS 服务器一般设在不同的服务器中。

现有两台 DNS 服务器，一台作为主 DNS 服务器，其 IP 地址为 192.168.13.100，其上建有 lnjg.edu.cn 域，建有 www.lnjg.edu.cn 和 ftp.lnjg.edu.cn 两条记录，分别对应 192.168.13.1 和 192.168.13.80；另一台作为辅助 DNS 服务器，其 IP 地址是 192.168.13.200，其上要建立辅助 DNS 服务器。下面简述辅助 DNS 服务器的配置过程。

**1. 主 DNS 服务器的配置**

在主 DNS 服务器上依次选择"开始"→"管理工具"→DNS，打开"DNS 管理器"。

在正向查找区域下的 lnjg.edu.cn 区域上右击鼠标，在弹出菜单中选择"属性"，选择"lnjg.edu.cn 属性"窗口中的"区域传送"选项卡，在其中选择"允许区域传送"及其下的"只允许到下列服务器"选项。单击"编辑"按钮，输入辅助 DNS 服务器的 IP 地址，服务器会自动进行连通性测试，检测出辅助 DNS 服务器的名称，如图 9-24 所示。

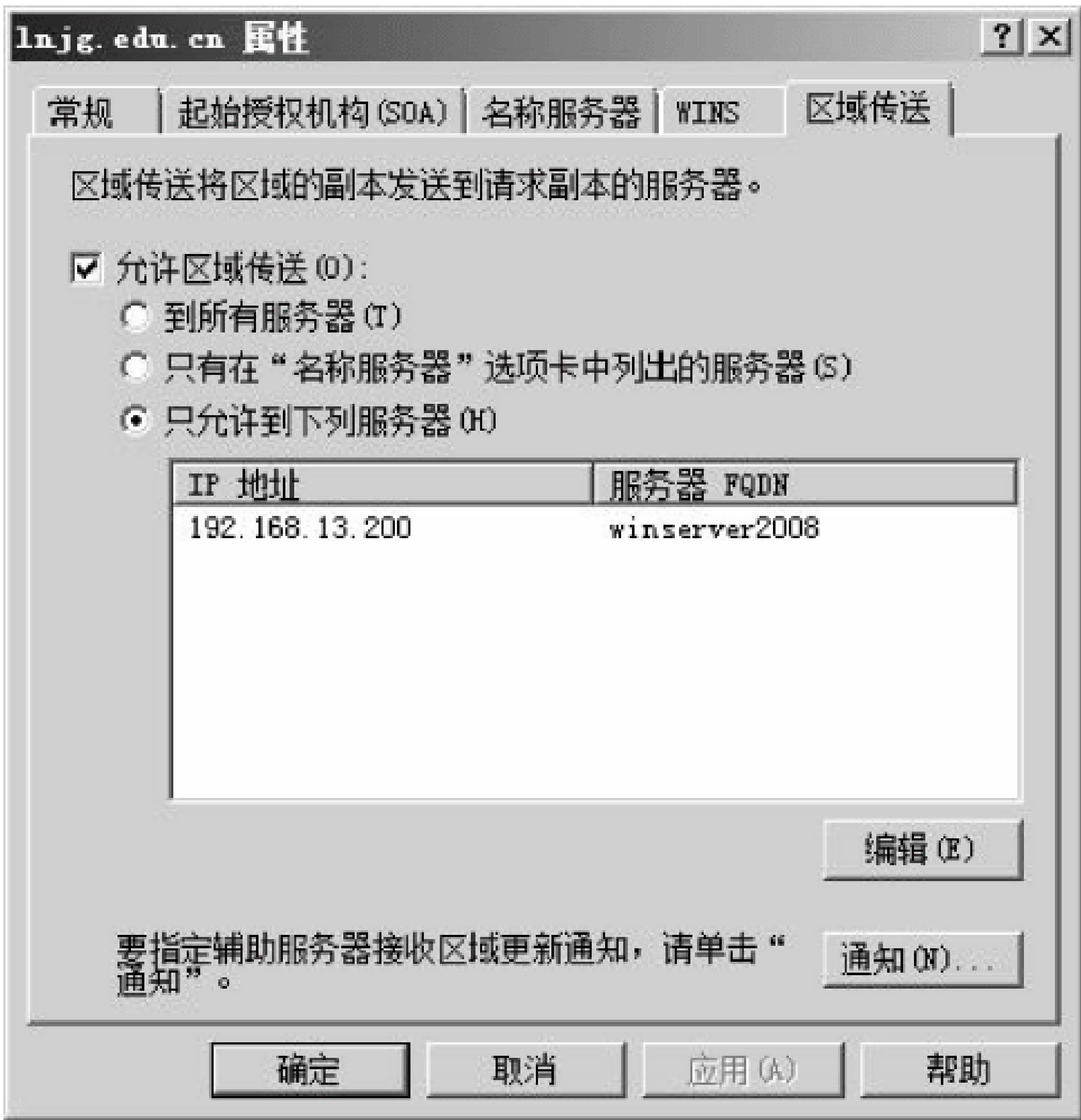



图 9-24　主 DNS 服务器设置区域传送

在主 DNS 服务器的反向查找域下的 13.168.192.in-addr.arpa 上右击，在弹出菜单上选择"属性"，在打开的属性窗口中，选择"区域传送"选项卡，选择"允许区域传送"及其下的

“只允许到下列服务器”选项。单击“编辑”按钮，输入辅助 DNS 服务器的 IP 地址，单击“确定”。此过程和上面的正向查找区域传送设置非常类似。

**2. 辅助 DNS 服务器的正向查找区域的设置**

步骤 1：在辅助 DNS 服务器上，依次选择“开始”→“管理工具”→DNS，打开“DNS 管理器”，右击“正向查找区域”，在弹出菜单中选择“新建区域”，在新建区域向导的“区域类型”选项中，选择“辅助区域”。单击“下一步”，如图 9-25 所示。

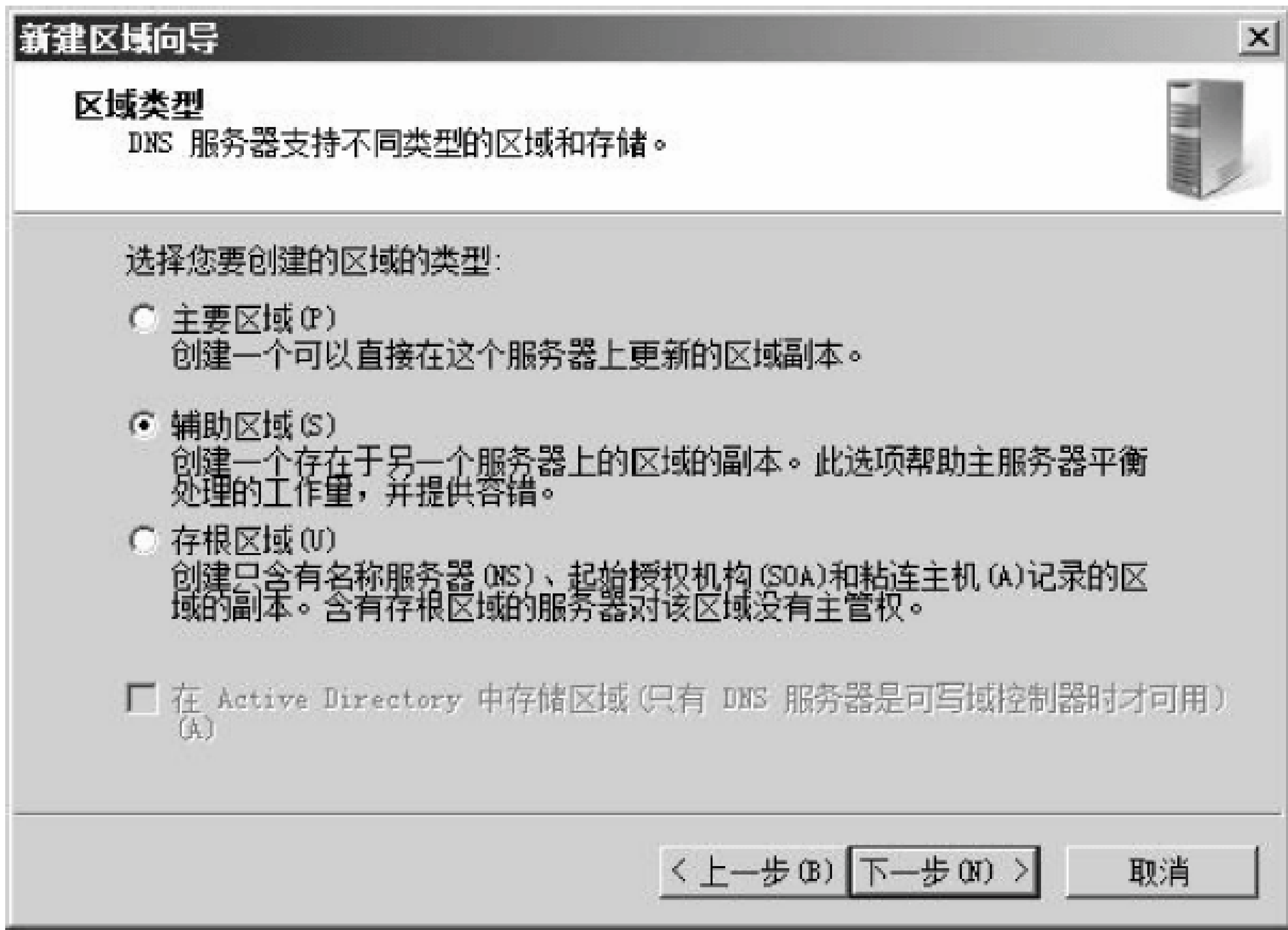



图 9-25 建立辅助区域

步骤 2：在新建区域向导的“区域名称”窗口中，输入区域名称，这里输入值为主 DNS 服务器相同的 lnjg.edu.cn。单击“下一步”，如图 9-26 所示。




图 9-26 辅助区域的名称

步骤 3：在新建区域向导的“主 DNS 服务器”窗口中，输入主 DNS 服务器的 IP 地址，如图 9-27 所示。

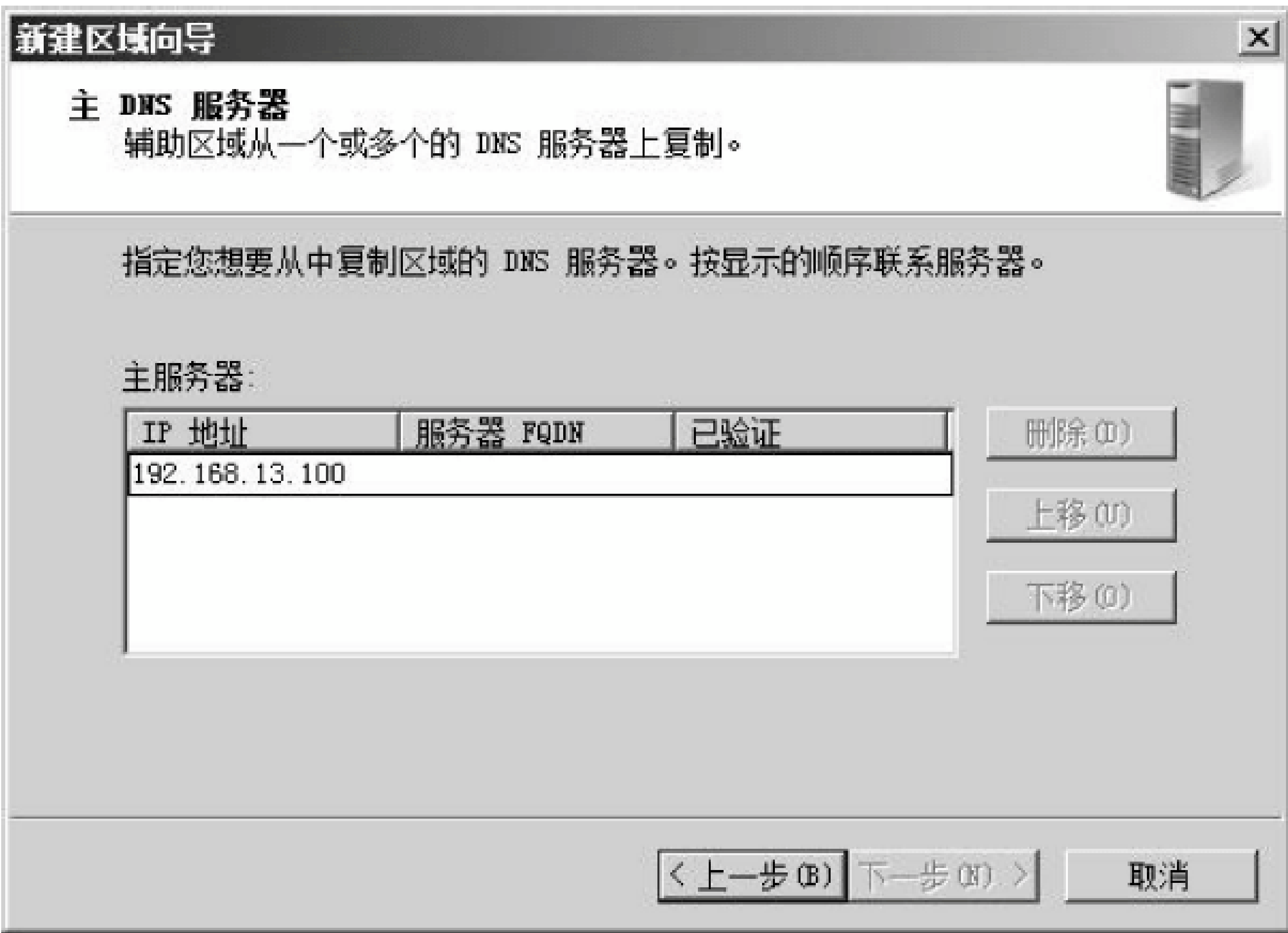



图 9-27　设置主 DNS 服务器的 IP 地址

**3. 辅助 DNS 服务器的反向查找区域的设置**

步骤 1：在辅助 DNS 服务器的“DNS 管理器”窗口中，右击“反向查找区域”，在弹出菜单中选择“新建区域”，在新建区域向导的“区域类型”选选项中，选择“辅助区域”。单击“下一步”按钮。

步骤 2：在新建区域向导的“反向查找区域名称”窗口中，选择“IPv4 反向查找区域”。单击“下一步”按钮，如图 9-28 所示。




图 9-28　反向查找区域名称

步骤 3：在新建区域向导的“反向查找区域名称”窗口中，输入网络 ID：192.168.13，这里与主 DNS 服务器的网络 ID 相同。单击“下一步”，如图 9-29 所示。

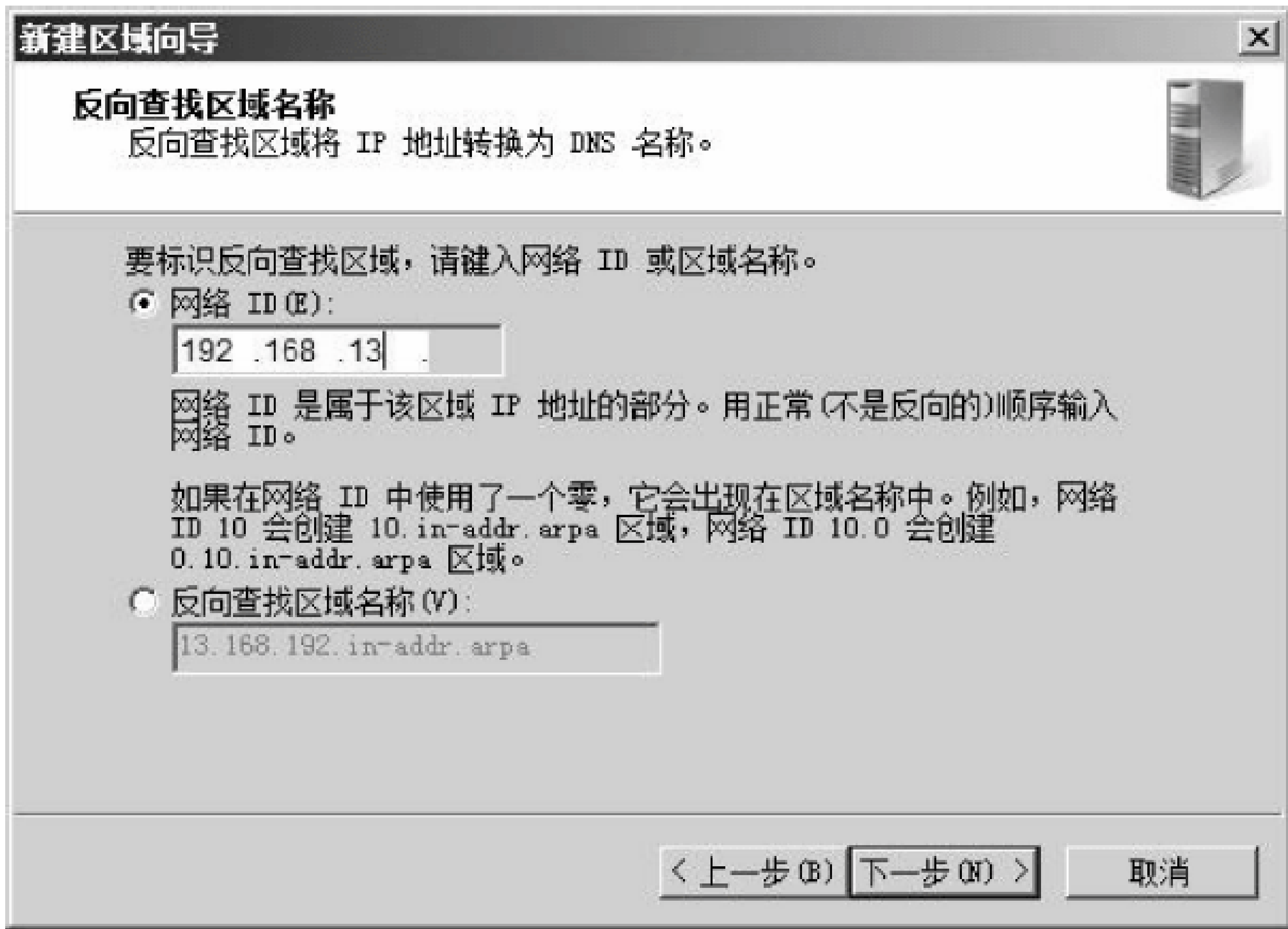



图 9-29　反向查找区域名称

步骤 4：在新建区域向导的“主 DNS 服务器”窗口中，输入主 DNS 服务器的 IP 地址 192.168.13.100，如图 9-30 所示。

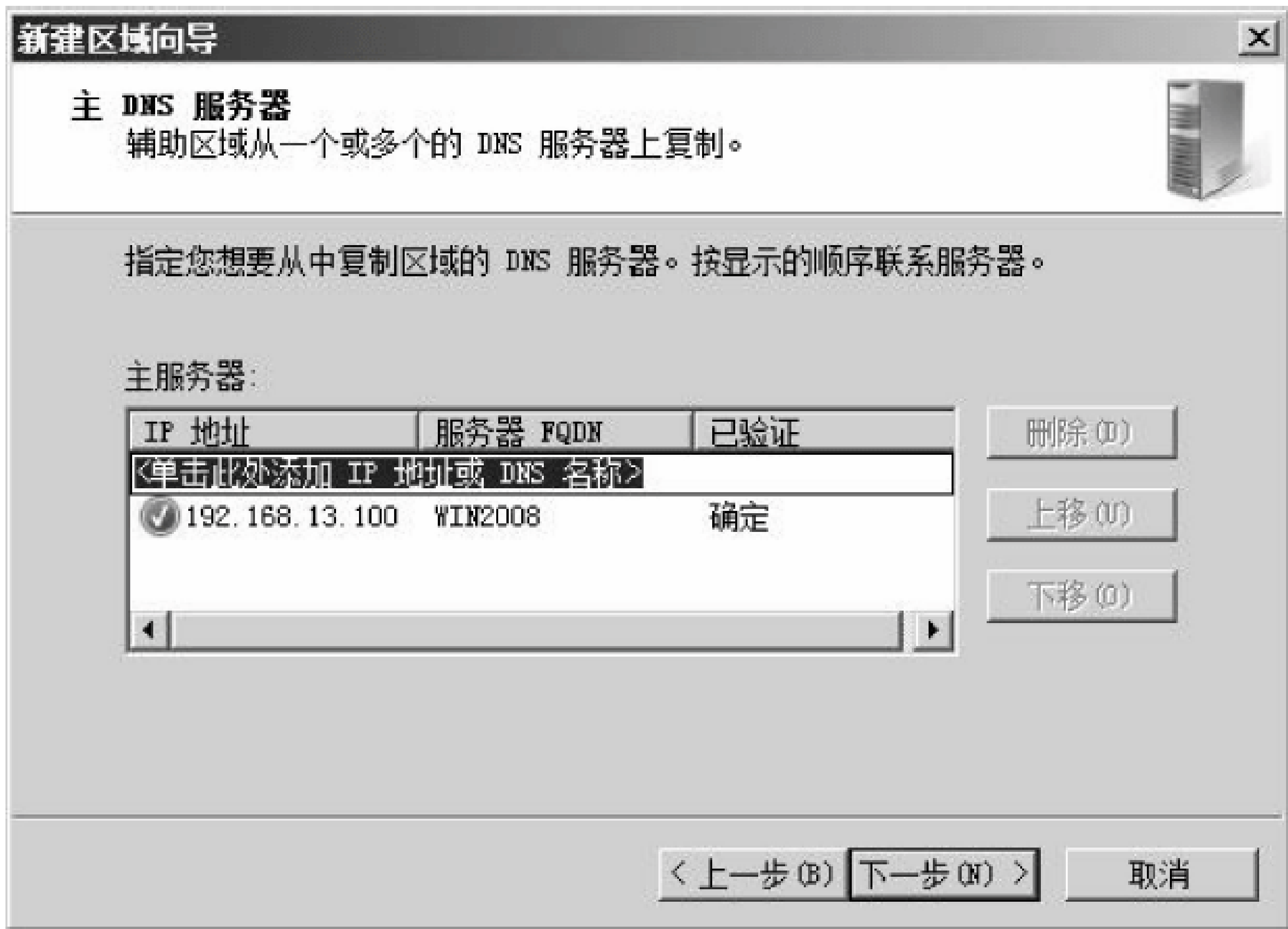



图 9-30　主 DNS 服务器的 IP 地址

步骤 5：在新建区域向导窗口中，单击“完成”，这时可以看到建立完成的辅助区域。

步骤 6：在 DNS 管理窗口中，右击新建立的“lnjg.edu.cn”区域，选择“从主服务器重新加载”，完成从主 DNS 服务器到辅助 DNS 服务器的数据传输，如图 9-31 所示。

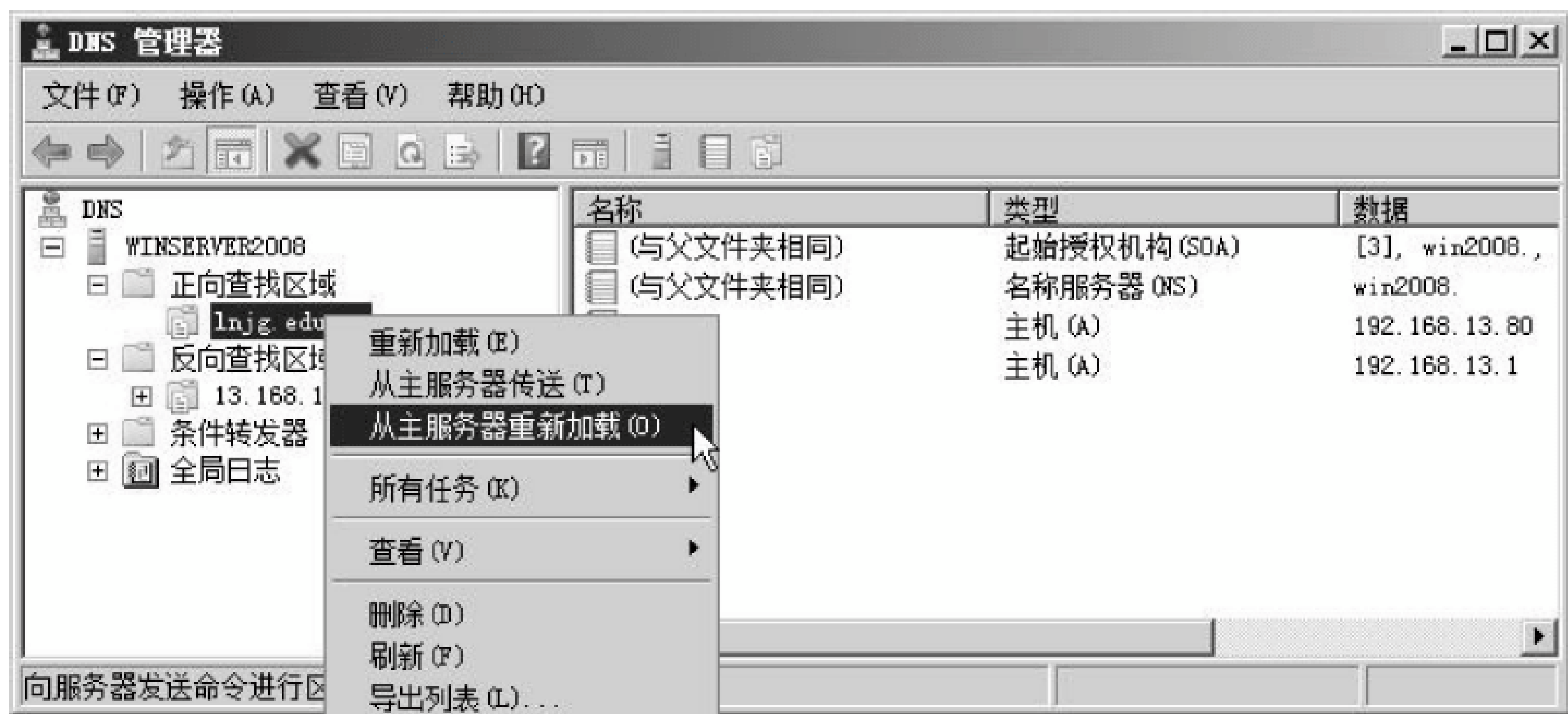



图 9-31　从主 DNS 服务器加载数据

# 实验 14　DNS 服务器的配置

**1. 实验目标**

(1) 配置主 DNS 服务器，辅助 DNS 服务器。

(2) 测试 DNS 服务器配置的正确性。

**2. 实验准备**

两台安装了 Windows Server 2008 的机器，一台客户机；或者一台安装了虚拟机的性能较好的计算机。

**3. 实验内容**

(1) 完成本章所有 DNS 服务器的配置实例。

(2) 假设已经注册了域名 abc.com，主 DNS 服务器的 IP 地址为 192.168.1.1，辅助 DNS 服务器的 IP 地址为 192.168.1.2。WWW 服务器的 IP 为 192.168.1.10，FTP 服务器的 IP 地址为 192.168.1.20。

要求：配置主 DNS 服务器，能解析 WWW 和 FTP 服务器的域名，配置辅助 DNS 服务器，实现与主 DNS 服务器的区域数据的传输。在客户端实现对 WWW 和 FTP 服务器域名的查找。

# 思考与练习

**一、填空题**

1. 通过 DNS，用户可以使用友好的名称查找________和服务在网络上的位置。

2. DNS 名称分为多个部分，各部分之间用________分隔。

3. 域名空间中处于最顶层的是________。

## 二、选择题

1. DNS 指针记录的标志是(　　)。
   A. A　　B. PTR　　C. CNAME　　D. NS
2. 以下（　　）命令可以测试 DNS 服务器的工作状态。
   A. ig　　B. host　　C. nslookup　　D. named-check
3. 在 DNS 中根域名文件是(　　)。
   A. root. dns　　B. local. dns　　C. *. arpa　　D. .(点)
4. 测试 DNS 主要使用以下(　　)命令。
   A. Ping　　B. IPconfig　　C. nslookup　　D. Winipcfg
5. 应用层 DNS 协议主要用于实现的网络服务功能是(　　)。
   A. 网络设备名字到 IP 地址的映射　　B. 网络硬件地址到 IP 地址的映射
   C. 进程地址到 IP 地址的映射　　D. 用户名到进程地址的映射
6. 在 DNS 正向查找中,查找模式有两种：一种是递归查找；另一种是(　　)。
   A. 迭代查找　　B. 反向查找　　C. 正向查询　　D. 回归查找
7. 域名最左边的是(　　),其余部分是该主机所属的 DNS 域。
   A. 实际地名　　B. 主机名　　C. 计算机名　　D. 服务端

## 三、问答题

1. 什么是 DNS? 它的主要作用是什么?
2. DNS 服务器主要有哪些类型?
3. DNS 查找模式有哪两种? 请简述其工作过程。
4. DNS 区域文件中有哪些记录?

第 10 章

# DHCP 服务器的配置与管理

## 10.1 DHCP 概 述

### 10.1.1 DHCP 简 介

在 Internet 网络中，每台主机都有一个确定的 IP 地址，以实现网络的通信与资源共享。IP 地址等网络信息的配置方式有两种：一种是静态配置；另一种是动态配置。在一个大型的网络中进行网络 IP 地址等信息的配置是比较困难的，网络管理员的工作量会比较大，这也会造成网络 IP 地址冲突的问题，影响网络用户对网络资源的利用。这时人们就想到了进行网络信息的动态配置，DHCP 技术应运而生。

DHCP(Dynamic Host Configuration Protocol，动态主机配置协议)是计算机网络应用层的一个重要服务，能够为连接到 TCP/IP 网络的系统提供配置信息，包括 IP 地址、子网掩码、网关、DNS 服务器地址等网络信息。DHCP 服务器分配给客户端的 IP 地址不是永久的，而是临时租借的。这样做的好处是：第一，可以解决 IP 地址不够用的问题。因为 IPv4 的地址空间是有限的，如果给每一个主机和网络设备的端口都分配一个静态的 IP 地址，显然，IPv4 的地址空间是不够用的。采用动态分配技术，服务器把 IP 地址动态地分配给客户端，当客户端不再需要时，服务器把 IP 地址收回，重新分配给其他客户使用。第二，采用动态分配客户端的 IP 地址、子网掩码、网关地址、DNS 服务器地址等网络属性，可以大减少网络管理员的工作量，也减少了网络 IP 地址冲突的机会。

DHCP 服务适用的场合：

(1) 网络规模比较大。因为网络规模比较大，网络中的主机比较多，为了给网络中的每台主机设置 IP 地址，网络管理员工作量巨大，这时使用 DHCP 服务可以大大减轻网络管理员的工作负担。

(2) 网络 IP 地址不够用。一个网络规模比较巨大，用户也较多，而这个网络获得的 IP 地址却不够用，并且用户同时上网的可能性较小，这时使用 DHCP 服务，可以充分利用 IP 地址。

(3) 网络中经常更改上网地点的客户机较多。因为经常更换上网地点，若采用静态 IP 方式，每次更换上网地点，都需要修改客户机的网络设置，给客户带来很大的不便，这时使用 DHCP 可以给客户带来很大的方便。

### 10.1.2 DHCP 的工作原理

DHCP 服务采用客户机/服务器(Client/Server,C/S)工作模式。网络管理员设立一个或多个 DHCP 服务器,并以租约的形式向 DHCP 客户端提供地址配置。DHCP 服务器中维护着一个数据库,这个数据库包括的信息有:可以分配给客户的有效地址的 IP 地址池、地址租借的持续时间、保留给特定用户的网络地址等信息。

**1. DHCP 客户机首次获得 IP 租约**

DHCP 服务采用 UDP 协议,其中 DHCP 服务器采用 67 号端口,DHCP 客户端采用 68 号端口,DHCP 客户端获得 IP 地址的过程又称为 DHCP 的租借过程,如图 10-1 所示。

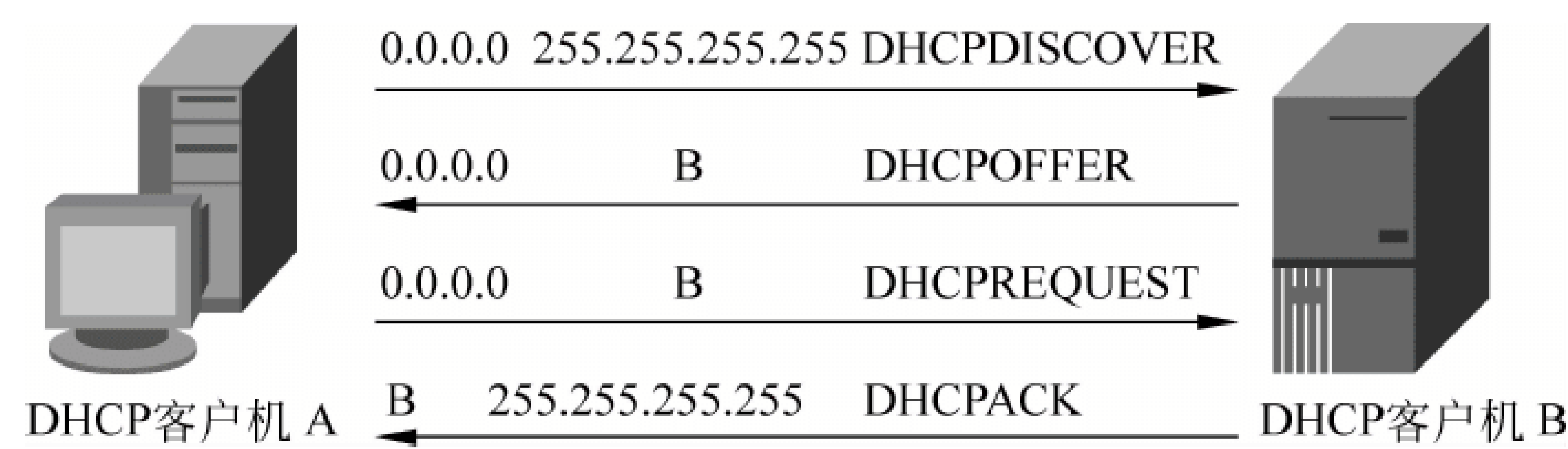



图 10-1 DHCP 租用过程

1) IP 租用请求

当 DHCP 客户机开机第一次以 DHCP 客户机身份登录网络,发现自己没有 IP 地址,并且还要使用网络资源时,便向网络发送一个 DHCPDISCOVER 广播包,该广播包的源地址为 0.0.0.0,目标地址为 255.255.255.255,这样的广播包会被同一网段的所有主机接收到。

2) IP 地址租用提供

网络中的 DHCP 服务器在收到上述的广播信息后,会从自己的 IP 地址池中随机地选择一个可用的 IP 地址,广播发送出去。这个 DHCPOFFER 广播包包括 IP 地址、子网掩码、租用期、DHCP 服务器的地址等信息。这个 IP 地址在未得到客户的租用之前会被服务器"隔离"开,以免被分配给其他用户。

3) IP 租用选择

DHCP 客户机收到网络上的多台 DHCP 服务器发送的信息后,会选择其中的一个 DHCPOFFER(通常会选择最先到达的那个),向网络发送一个 DHCPREQUEST 广播包,告诉所有的 DHCP 服务器它选择了哪一个服务器提供的 IP 地址,其他服务器则收回自己的 IP 地址。

4) IP 租用确认

当 DHCP 服务器收到 DHCP 客户机发送的 DHCPREQUEST 请求信息后,便向客户机发送一个 DHCPACK 信息,告诉 DHCP 客户机可以使用它提供的 IP 地址。客户机接收到确认信息后,便完成 IP 地址的租用过程。

**2. IP 地址的续租**

取得 IP 租约后，DHCP 客户机必须定期地向 DHCP 服务器续租，以免过期，服务器收回这个 IP 地址。

(1) DHCP 客户机使用这个 IP 达到租约的 50%时间时，客户机便以单播方式向服务器发送 DHCPREQUEST 消息，请求继续使用原先租得的 IP 地址。

(2) 若 DHCP 服务器收到续租请求后，没有拒绝的理由，便也以单播方式发出 DHCPACK 信息，DHCP 客户机收到确认信息后，继续使用原来的 IP 地址；若没有收到服务器的确认信息，DHCP 客户端继续使用该 IP，因为还未到期。若 DHCP 服务器不同意继续租借，则发送一个 DHCPNACK 否认信息，客户机必须停止使用该 IP，并开始新的申请过程。

(3) 若 DHCP 客户机一直没有收到服务器的回应信息，到 87.5%租期时，DHCP 客户机以广播方式发送 DHCPREQUEST 消息，并继续使用该 IP，直到租期已满，则以广播方式发送 DHCPDISCOVER 消息，重新开始新的一轮 IP 租约过程。

# 10.2　DHCP 服务器的安装与配置

## 10.2.1　DHCP 服务器的安装

安装和运行 DHCP 服务器需要具备一个静态 IP 地址和一组有效可供分配的 IP 地址以及相应的网络。下面详细说明 DHCP 服务器的安装与配置过程。

步骤 1：依次选择“开始”→“管理工具”→“服务器管理器”。打开“服务器管理器”窗口。

步骤 2：在“服务器管理器”窗口中，选择窗口左侧的“角色”选项，在右侧选择“添加角色”选项，如图 10-2 所示。

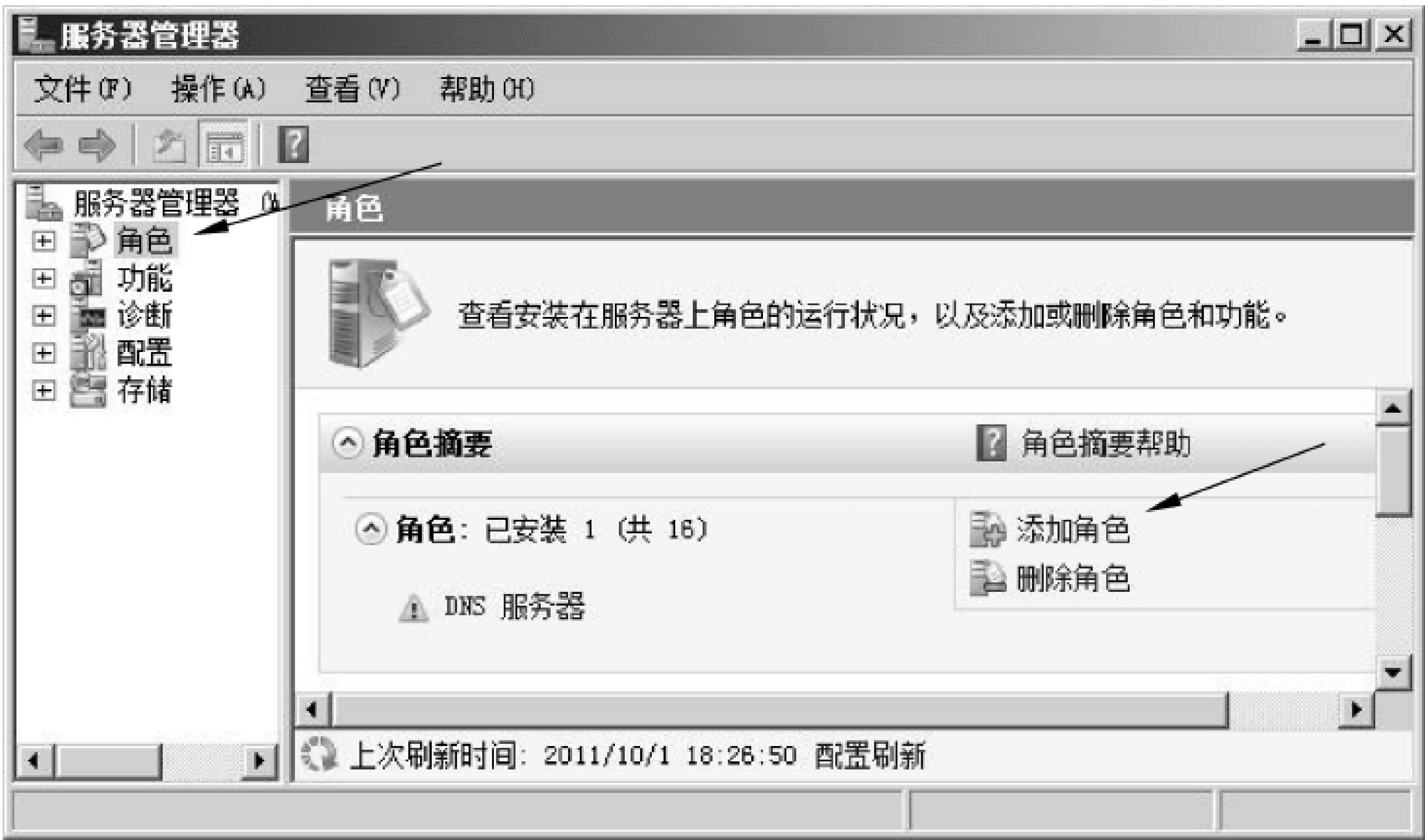



图 10-2　添加角色

步骤3：在弹出的窗口中单击“下一步”，进入到“选择服务器角色”步骤，在该步骤中，选中“DHCP服务器”选项，单击“下一步”按钮，如图10-3所示。




图10-3 选择服务器角色

步骤4：在“DHCP服务器简介”步骤，单击“下一步”按钮。

步骤5：在“服务器连接绑定”步骤，将把DHCP服务器与本服务器的静态IP进行绑定。如果有多个网络连接，向导会检测出来并列在网络连接中，选择向用户DHCP客户提供DHCP服务的连接，单击“下一步”按钮，如图10-4所示。

步骤6：在“IPv4服务器设置”步骤，在该步骤的父域中输入活动目录的域名。如果所在服务器中有域控制器，则向导自动检测出父域的域名。在“首选DNS服务器IPv4地址”中输入第一个DNS服务器的IP地址192.168.13.200，在“备用DNS服务器IPv4地址”文本框中输入备用DNS服务器的地址192.168.13.201。即使服务器不处于域环境中，也必须设父域名称，单击“下一步”按钮，如图10-5所示。

步骤7：“IPv4 WINS服务器设置”步骤中，指定是否需要使用WINS。目前大多数网络中已经不再使用WINS服务器，本步选择“此网络上的应用程序不需要WINS”，单击“下一步”按钮，如图10-6所示。

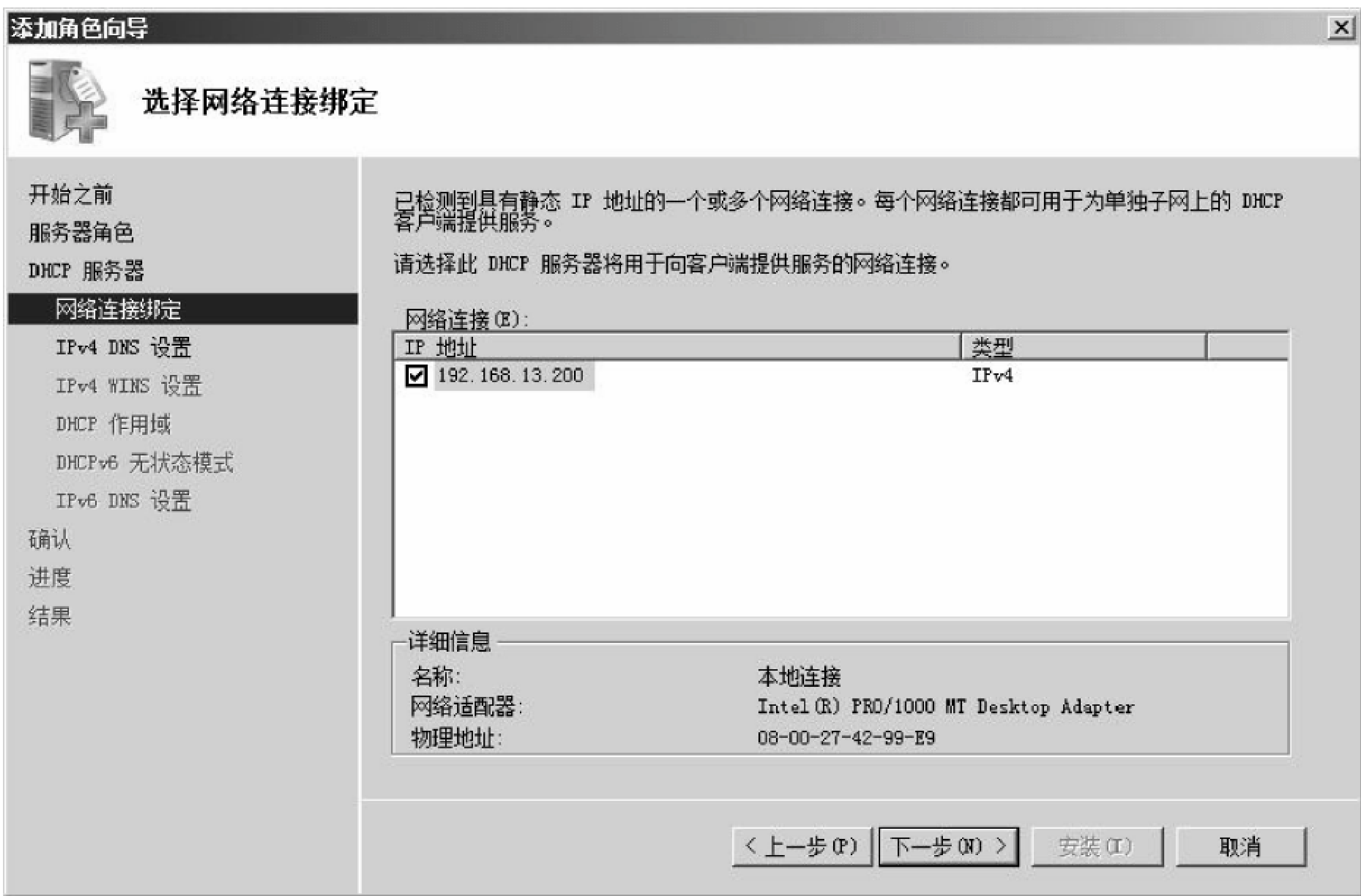



图 10-4　DHCP 服务器与网络连接的绑定

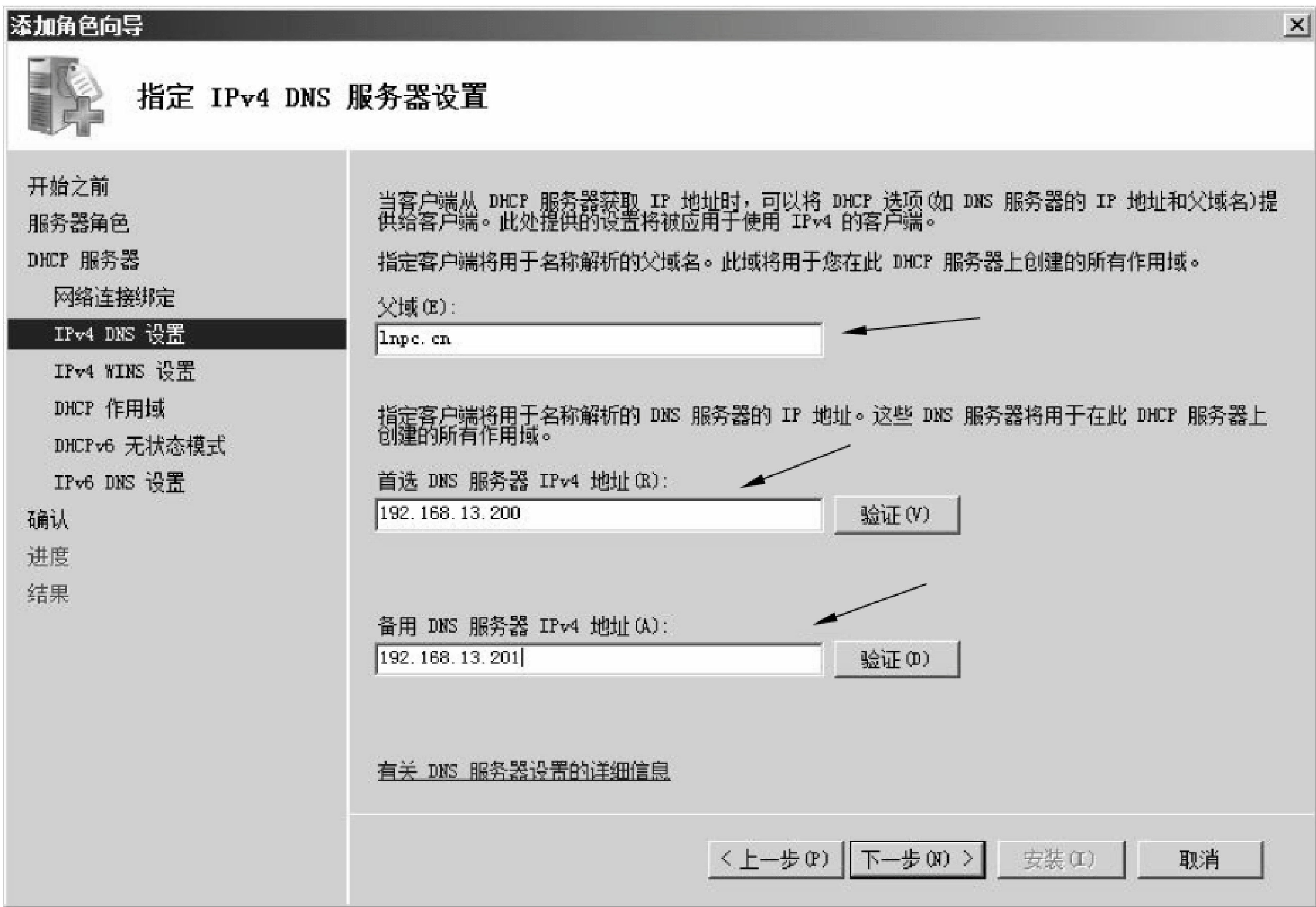



图 10-5　DNS 服务器设置

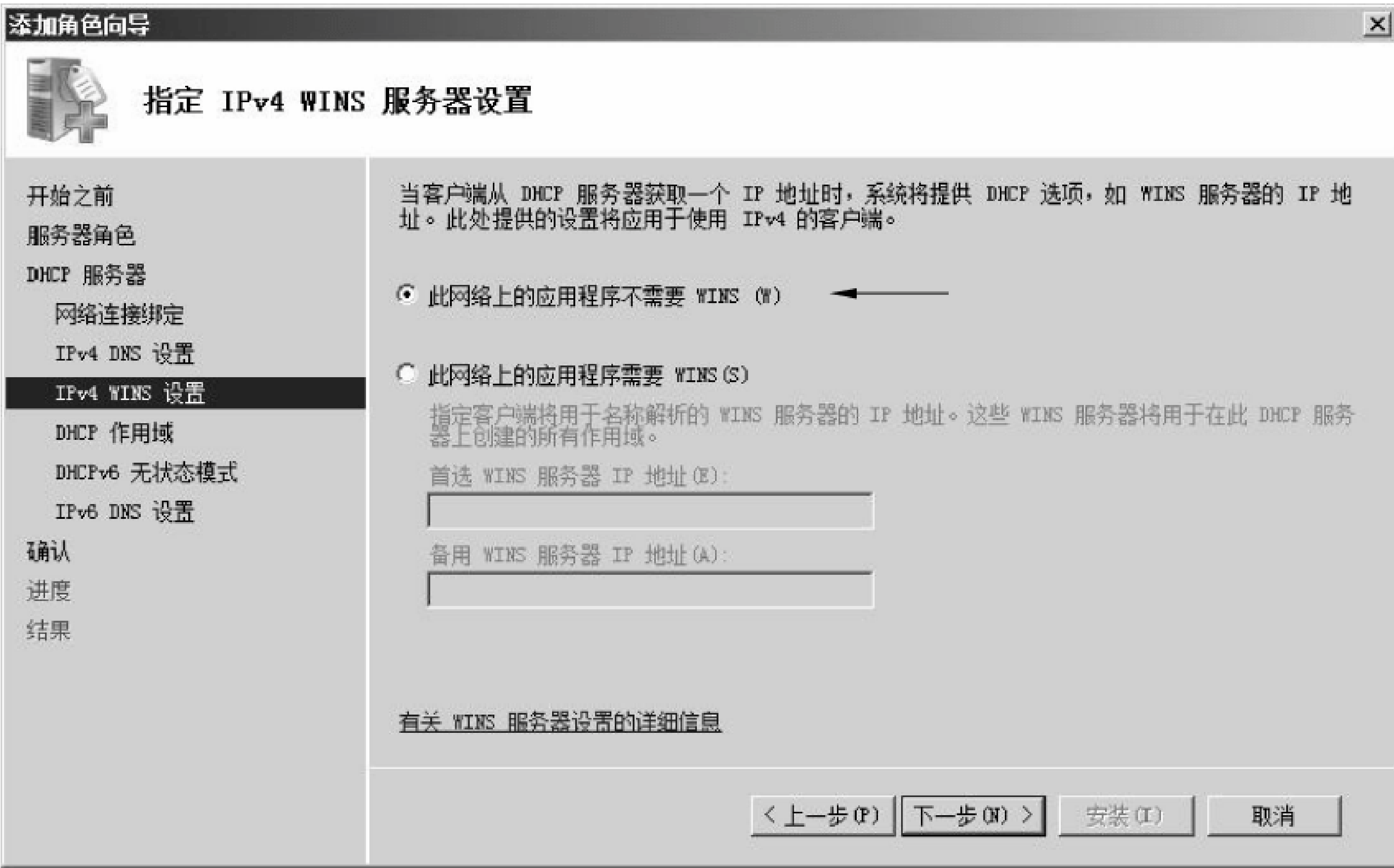



图 10-6　IPv4 WINS 设置

步骤 8：进入“添加作用域”步骤，此步骤用于指定 DHCP 服务器的作用域。也可在安装完成之后再设置，如图 10-7 所示。单击“添加”，打开“添加作用域”窗口，在这里可以输入一个 IP 地址段。单击“下一步”按钮。

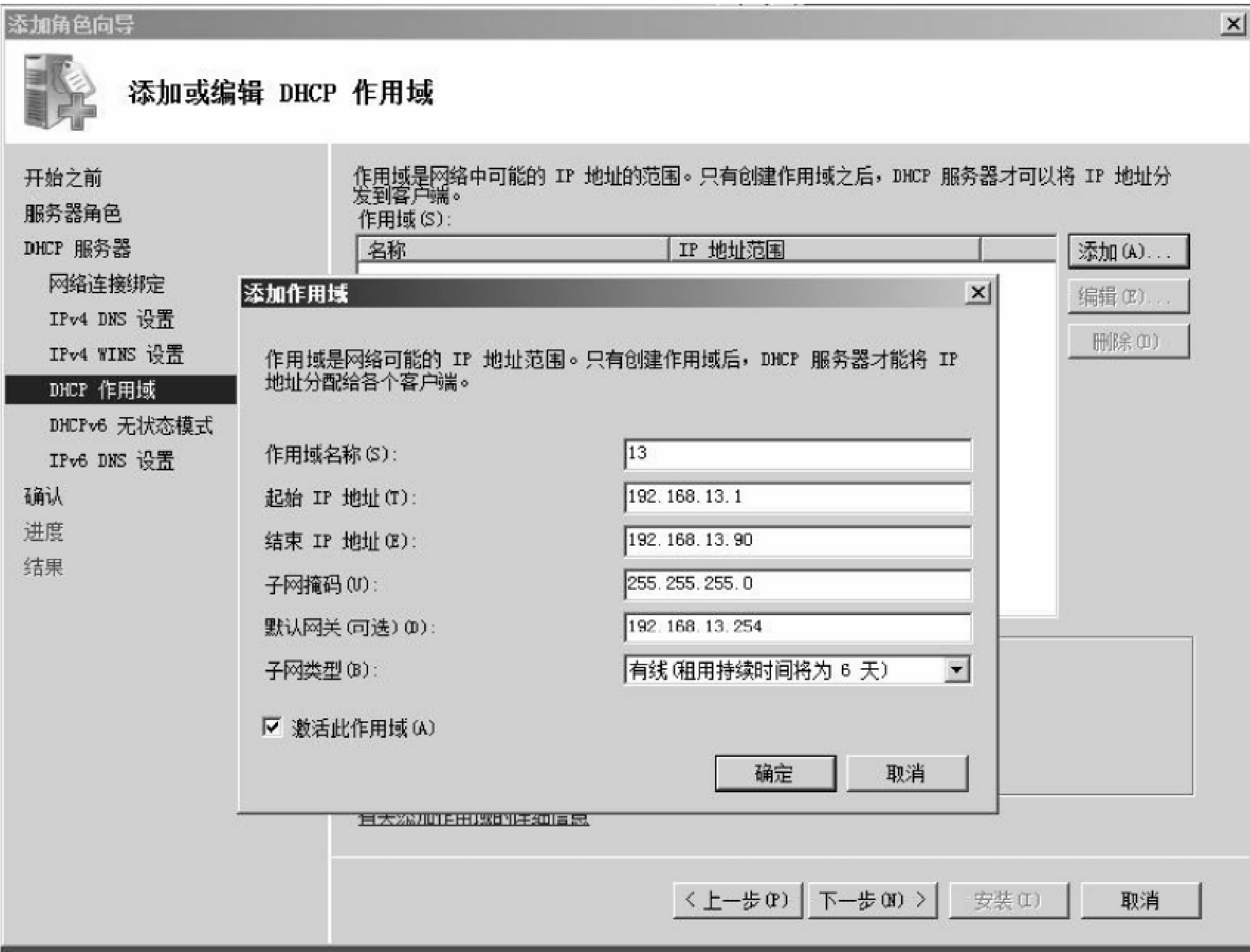



图 10-7　设置 DHCP 服务器的作用域

步骤 9：进入“配置 DHCPv6 无状态模式”步骤，因目前并未使用 IPv6，所以选择“对此服务器禁用 DHCPv6 无状态模式”，单击“下一步”按钮，如图 10-8 所示。

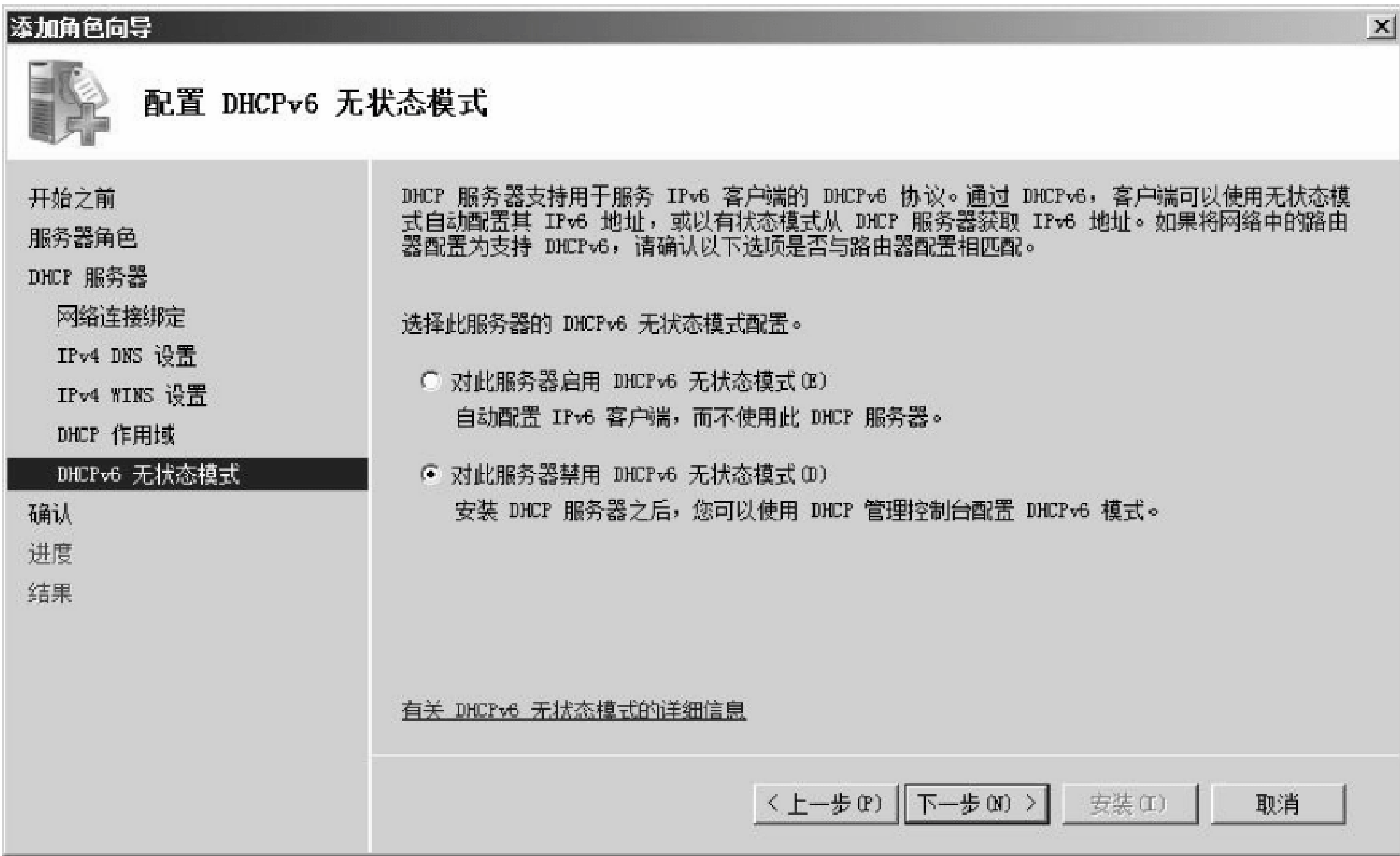



图 10-8　设置 DHCPv6 模式

步骤 10：在“确认”步骤，单击“安装”进行 DHCP 服务器的安装。

步骤 11：安装完成后，依次选择“开始”→“管理工具”→DHCP 命令，打开 DHCP 窗口，如图 10-9 所示。




图 10-9　DHCP 控制台

### 10.2.2 DHCP 服务器的配置

**1. 新建作用域**

作用域是网络中 DHCP 作用的范围，以确定分配给自己域内客户端 IP 地址的数量与范围。为了向不同网络提供不同的 IP 地址，需要创建不同的作用域。

步骤 1：打开“DHCP 控制台”，在左边的 IPv4 上右击，在弹出菜单中选择“新建作用域”，如图 10-10 所示。

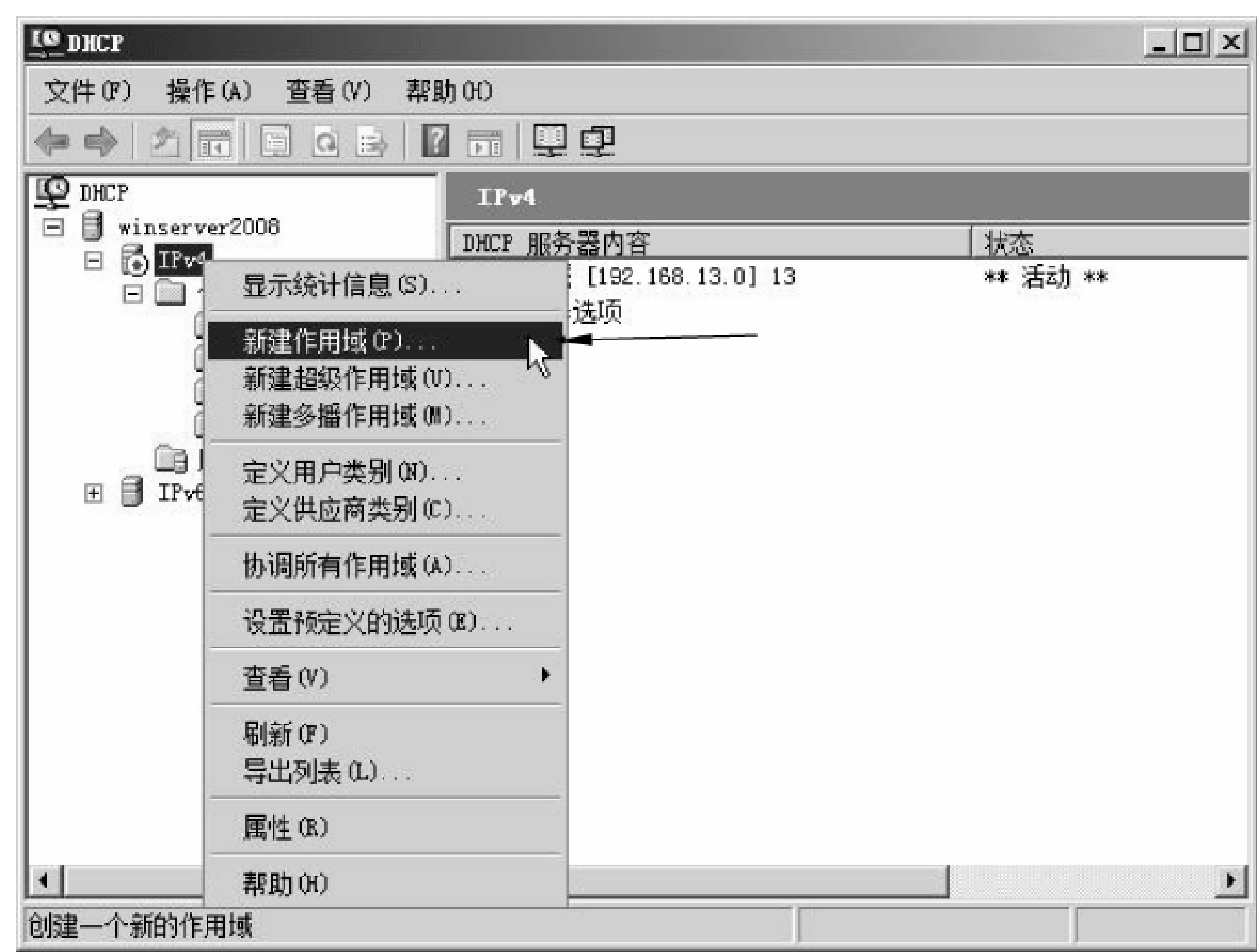



图 10-10 新建 DHCP 作用域

步骤 2：开始“新建作用域向导”，在欢迎界面中单击“下一步”按钮。

步骤 3：向导的“作用域名称”步骤中输入作用域名称，如图 10-11 所示。

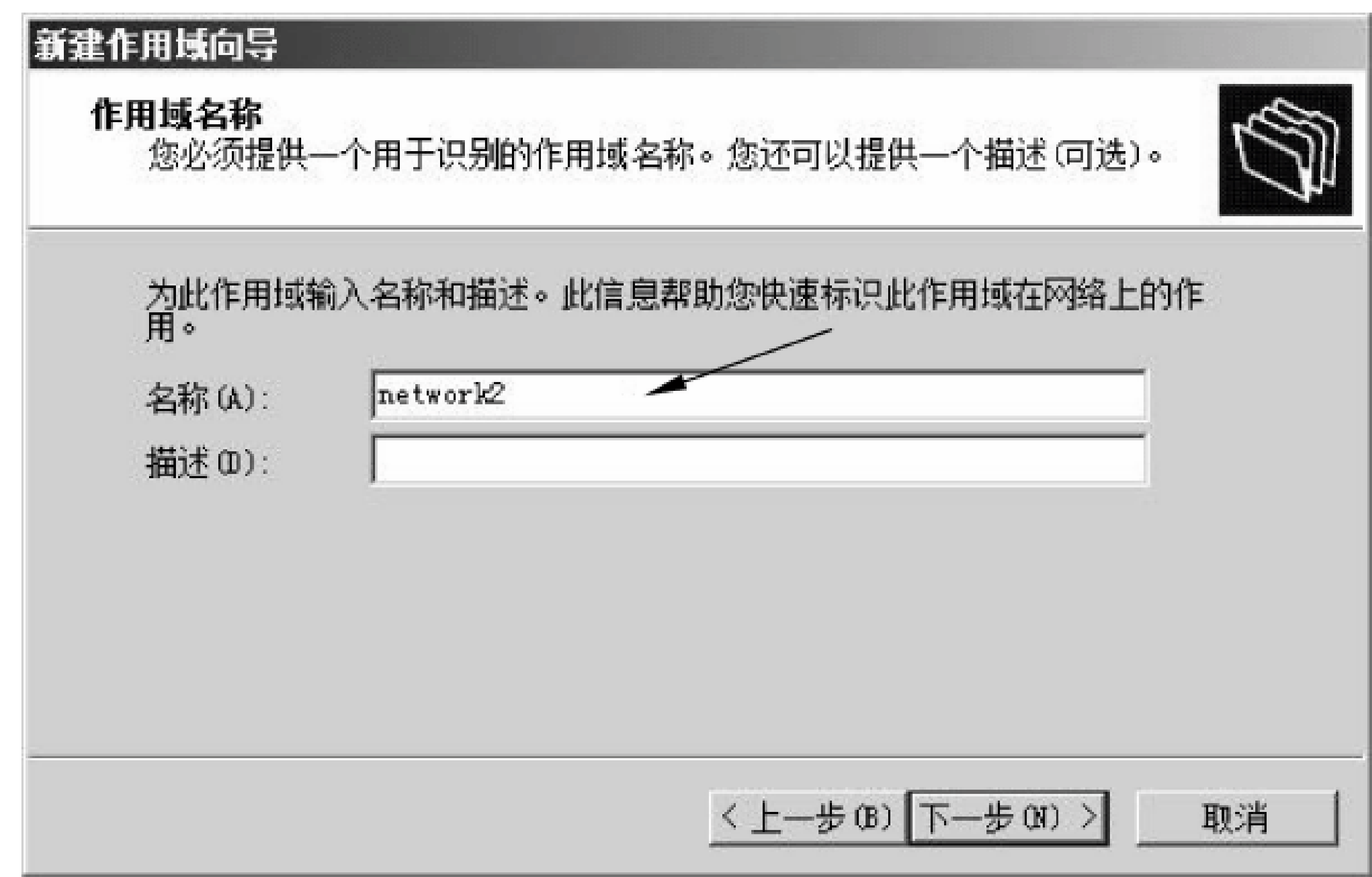



图 10-11 输入 DHCP 作用域名称

步骤4：在向导的“IP地址范围”步骤中，在“起始IP地址”栏中输入起始IP地址192.168.2.1，在结束IP地址栏中输入结束IP地址192.168.2.100，如图10-12所示。注意IP地址的类型和下面的子网掩码是否相符，如果不符，请修改。

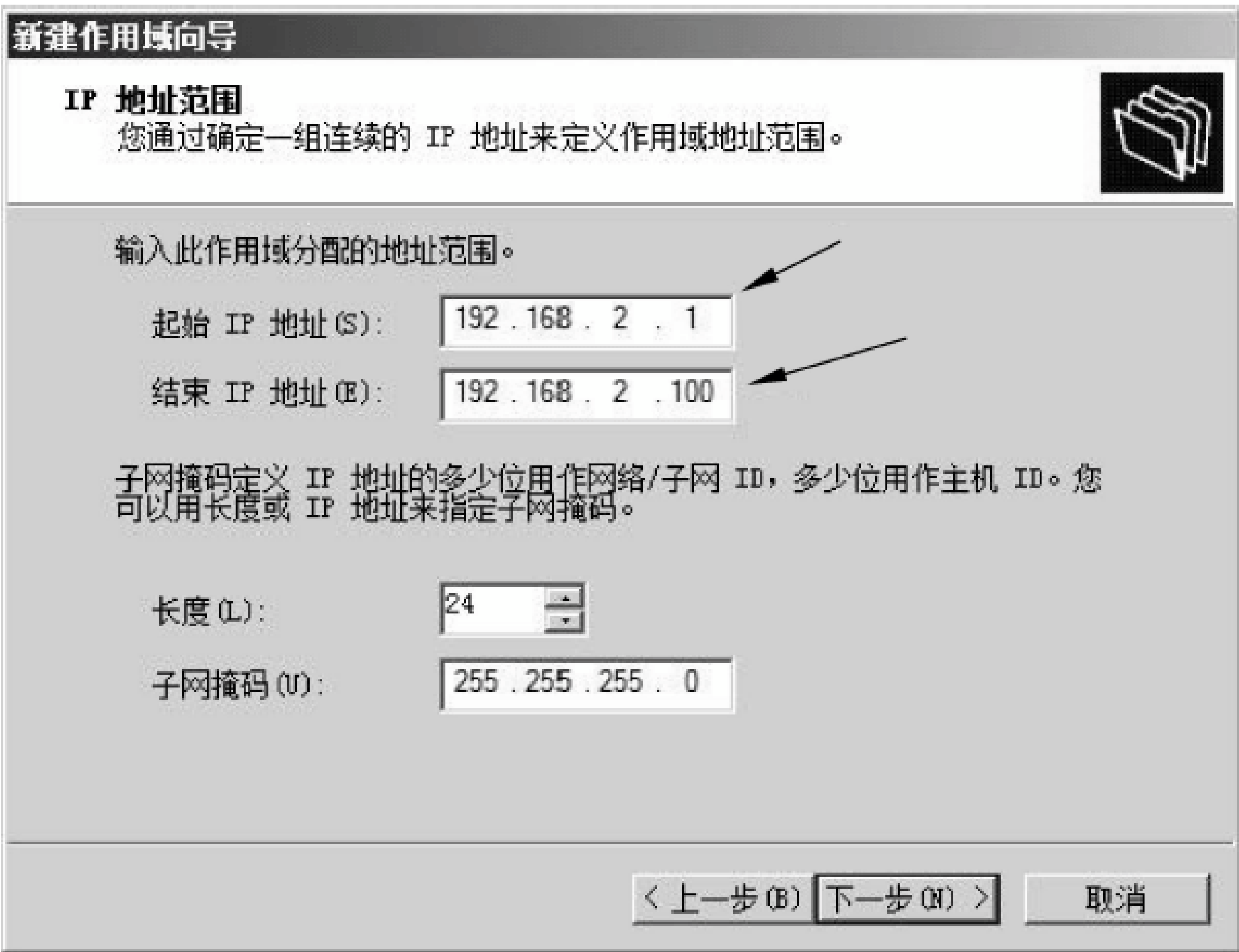



图10-12　设置DHCP作用域的IP范围

步骤5：在向导“添加排除”步骤中，设置不分配的IP地址，在起始IP地址中输入起始IP地址192.168.2.30，在结束IP地址栏中输入192.168.2.40，单击“添加”按钮，把要排除的IP地址添加到了下面的列表中。如果仅排除一个IP地址，只在起始IP地址栏中输入即可，如本例只排除192.168.2.80，如图输入即可。单击“下一步”按钮，如图10-13所示。

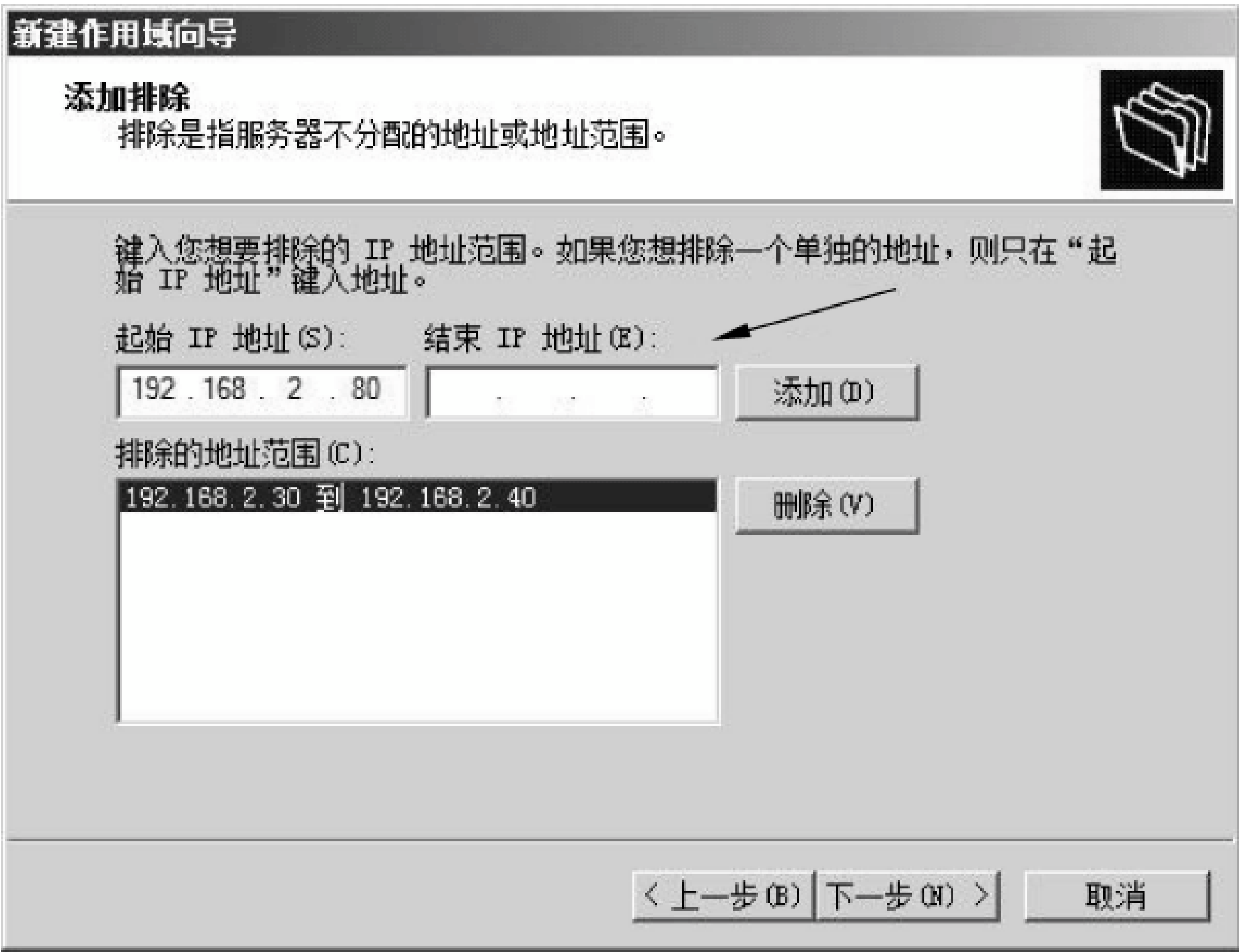



图10-13　为作用域添加排除

步骤 6：在向导的“租用期限”步骤中，设置租用期限，一般对于移动性比较大的网络中设置比较短的租用期比较好，对于移动性较小的网络可设置较长的租用期。默认租用期为 8 天，如图 10-14 所示。




图 10-14　设置作用域的租用期限

步骤 7：在向导的“配置 DHCP 选项”中，选择是否配置 DHCP 选项。包括默认网关、DNS 服务器、WINS 等设置，如图 10-15 所示。

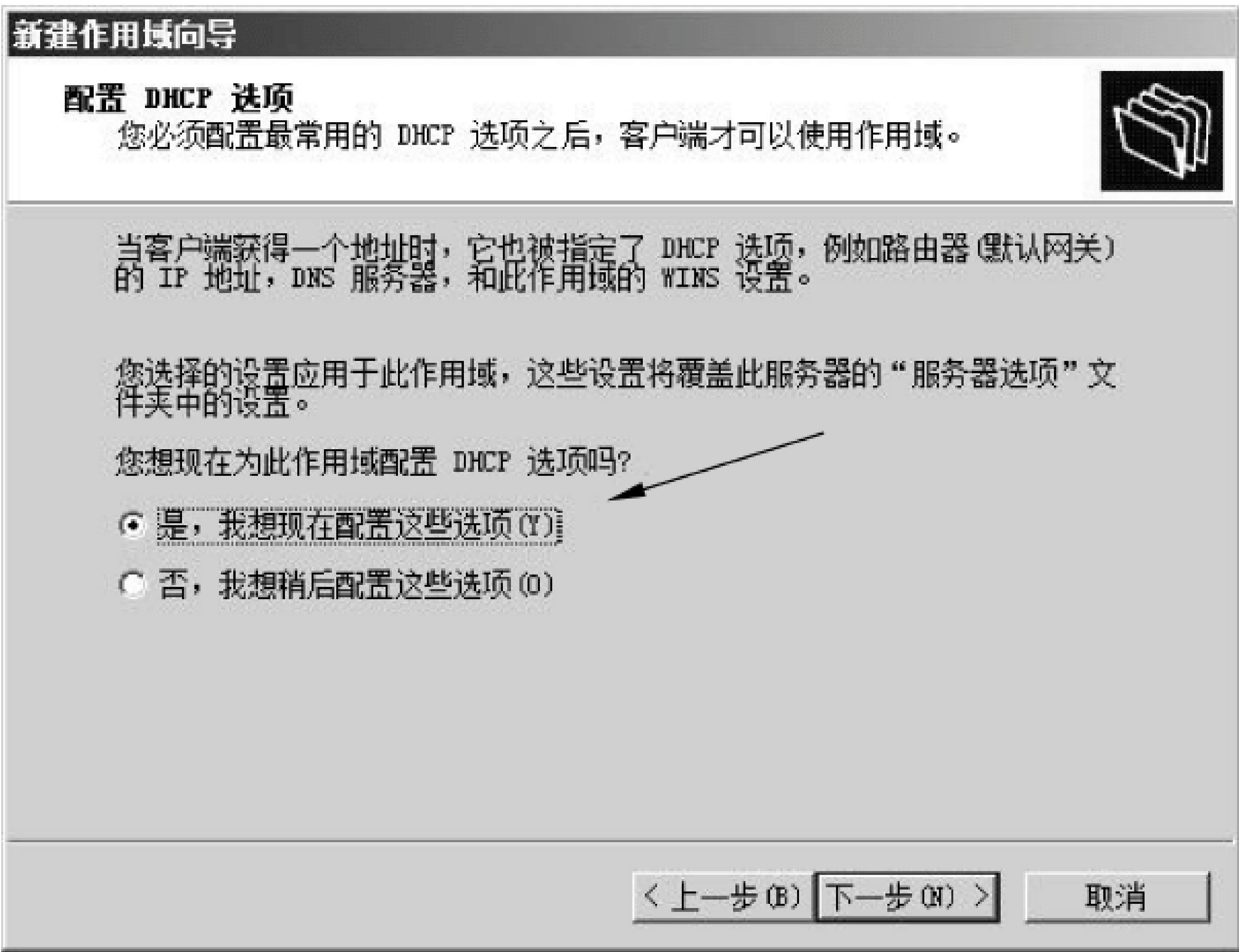



图 10-15　选择是否配置 DHCP 选项

步骤 8：在向导的“默认网络”步骤中，输入作用域的默认网关，这里的值要和网络的设置相对应，如图 10-16 所示。

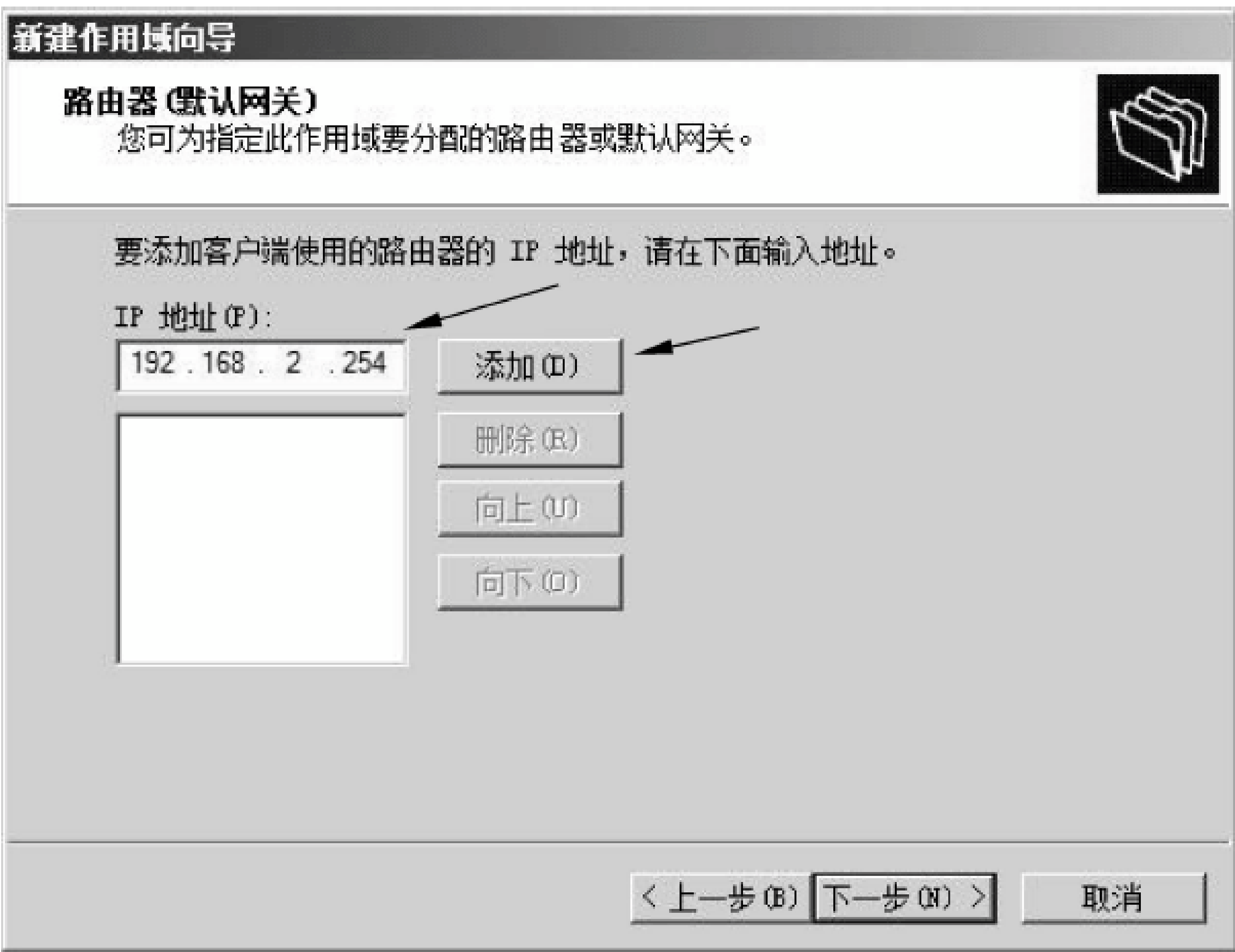



图 10-16　设置作用域的默认网关

步骤 9：向导的“域名称和 DNS 服务器”步骤，在父域栏中输入父域的名称 lnpc. cn，在“服务器名称”栏中输入服务器名称，单击解析即可解析出服务器的 IP 地址；也可以直接在 IP 地址栏中输入服务器的 IP 地址 192. 168. 13. 200，如图 10-17 所示。




图 10-17　设置作用域的父域及 DNS 服务器

步骤 10：进入向导的“WINS 服务器”步骤，设置 WINS 相关参数。这里不用设置直接单击“下一步”按钮。

步骤 11：进入向导的“激活作用域”步骤，作用域建立完成以后，激活才能发挥作用。选择相应选项后，单击“下一步”按钮，如图 10-18 所示。

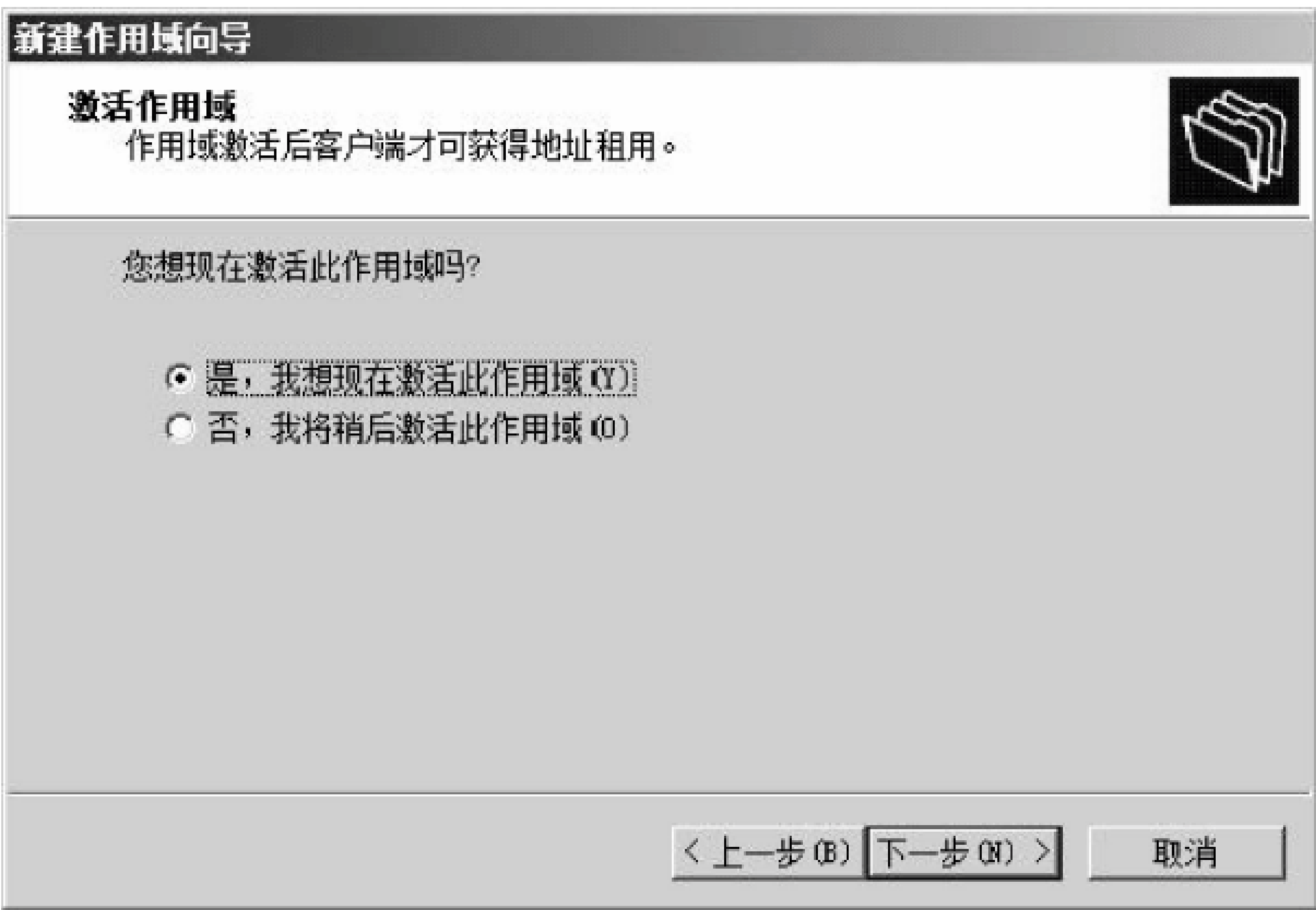



图 10-18　选择是否激活作用域

步骤 12：在向导的“完成”步骤，单击“完成”按钮，在 DHCP 管理控制窗口，可以看到相应的作用域。

**2. 保留特定的 IP 地址**

在配置 DHCP 服务器时，有时需要把某一特定的 IP 地址保留给某一客户让他长期使用。DHCP 服务器是通过客户机的 MAC 地址来识别客户的，然后把这个长期保留的 IP 地址分配给这个特殊的客户。

在 Windows 系列操作系统中，获得机器 MAC 地址的方法是：选择“开始”→“运行”，在找开的窗口中输入 cmd，打开命令行窗口，执行 ipconfig /all 即可查看当前计算机系统的网络配置，如图 10-19 所示。该客户机的 MAC 地址为 00-40-CA-D1-D9-C1。

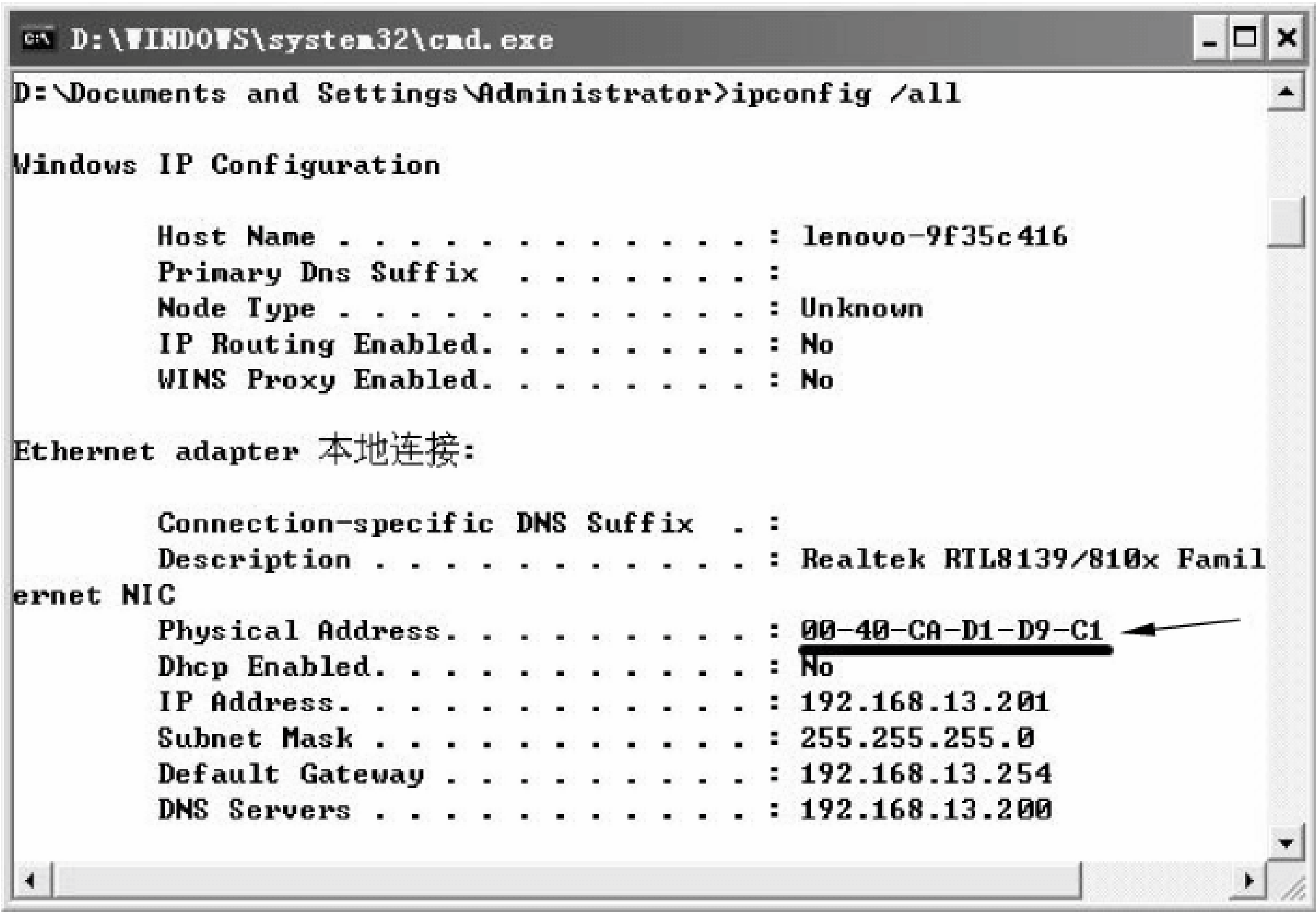



图 10-19　查看客户机的网络配置

在打开的 DHCP 管理控制窗口中，在作用域下的“保留”选项上右击，选择“新建保留”选项，如图 10-20 所示。

在打开的“新建保留”窗口中，输入保留的名称，这个名称可以随意命名，只要可以唯一标识该保留即可。保留的 IP 地址，本例中保留 192.168.13.1；客户机的 MAC 地址，本例中客户机的 MAC 地址为 00-40-CA-D1-D9-C1；在支持的类型中，BOOTP 是一个基于 IP/UDP 的协议，它可以让无盘工作站从一个中心服务器上获得 IP 地址，为局域网中的无盘工作站分配动态 IP 地址，这里要选择仅 DHCP 或其他类型。单击“添加”即可执行添加动作，添加结束后，单击“关闭”按钮，结束添加过程，如图 10-21 所示。




图 10-20　新建保留

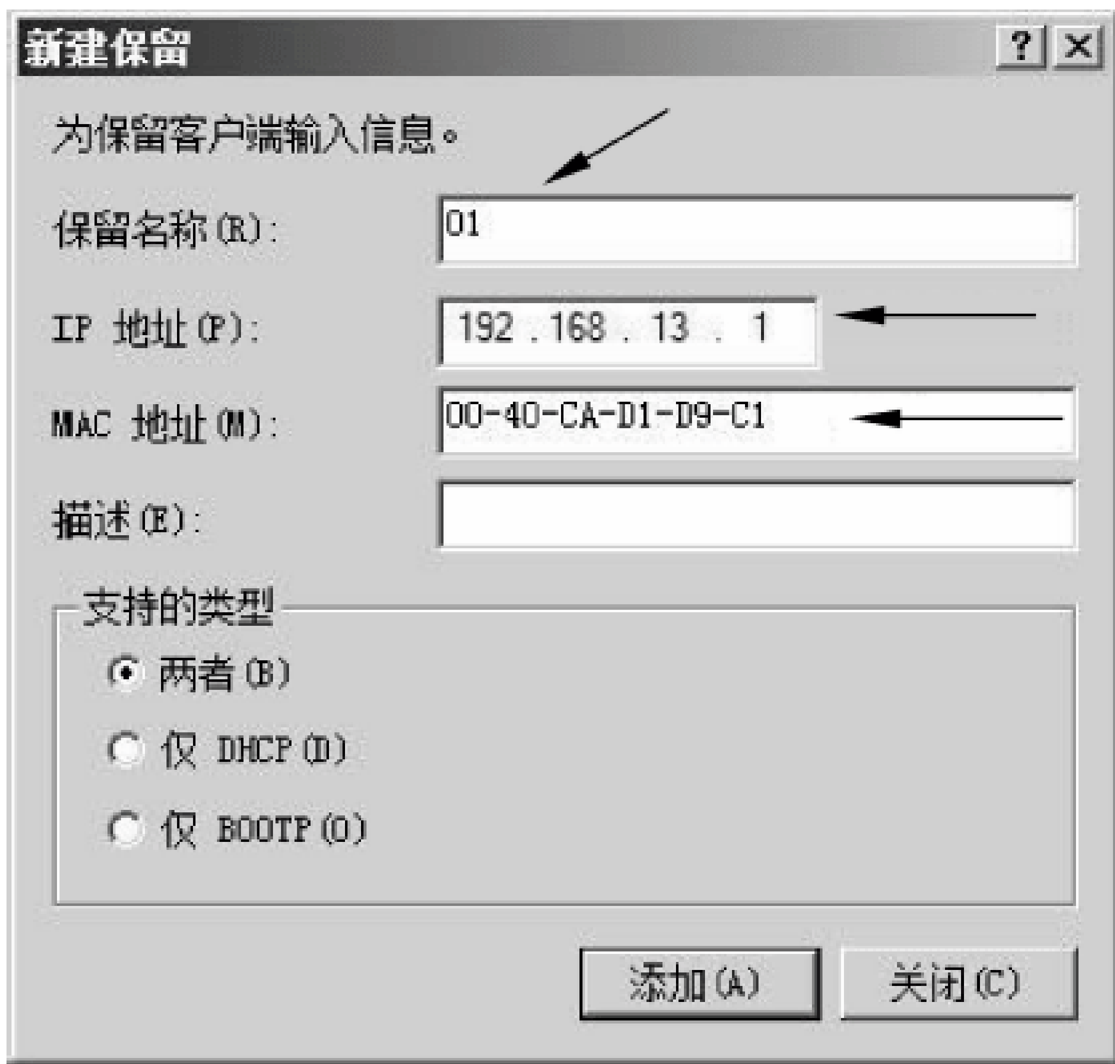



图 10-21　为保留输入信息

### 3．DHCP 的地址排除

从 DHCP 服务器的作用域中排除一些 IP 地址，使这些 IP 地址不参加地址分配，而使用静态配置的方法设置一些服务器、路由器等设备，让这些设备长期使用被排除的 IP 地址。除了新建作用域时指定排除 IP 地址方法外，也可以在配置完作用域后，再添加地址排除。下面简要介绍地址排除的方法。

在 DHCP 管理控制窗口左侧“作用域”下的“地址池”上右击，选择弹出菜单“新建排除范围”，如图 10-22 所示。

在打开的“添加排除”窗口中，输入排除的 IP 地址范围，单击“添加”按钮，即完成地址排除工作，如图 10-23 所示。

### 4．配置作用域和服务器选项

DHCP 服务器除了给客户端分配 IP 地址外，还配置其他一些选项，如默认网关、DNS 服务器、WINS 等。因此，有时需要维护作用域和服务器的一些选项。作用域的选项作用于从它这儿分配 IP 的客户机，服务器的选项作用于从这台服务器获取 IP 地址的客户机，作用域的优先级高于服务器的优先组。




图 10-22 新建排除范围

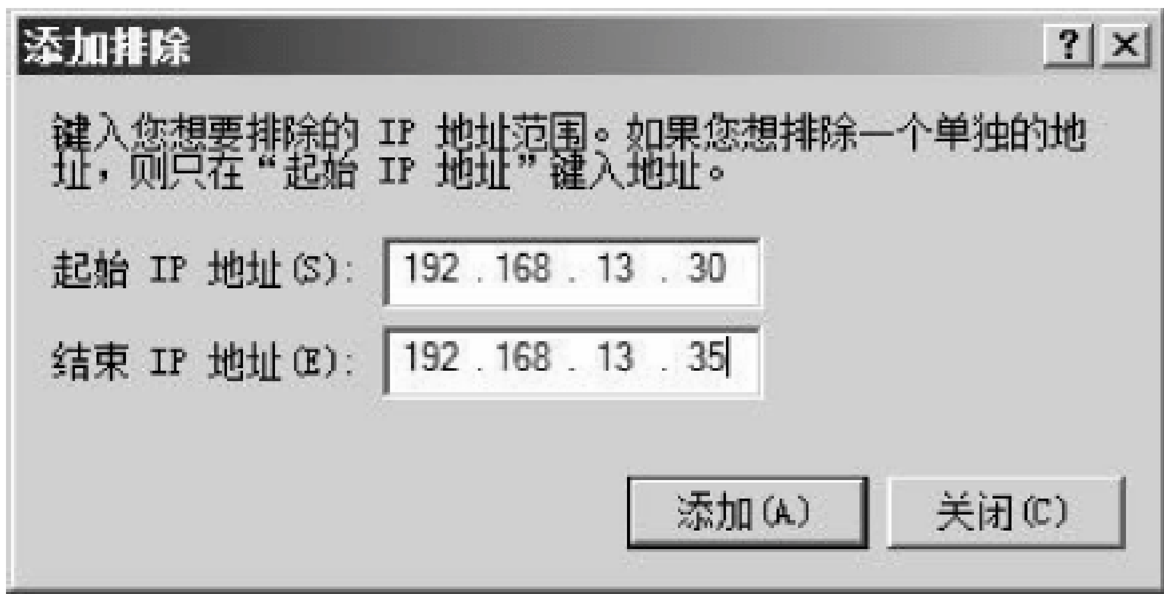



图 10-23 添加排除

1）服务器选项的设置

步骤 1：依次选择“开始”→“管理工具”→DHCP，打开 DHCP 管理控制平台，右击 IPv4 下的“服务器选项”，在弹出菜单中选择“配置选项”，如图 10-24 所示。




图 10-24 配置 DHCP 服务器选项

步骤 2：在打开的窗口中，在“高级”选项卡中，可以设置“供应商类别”和“用户类型”。“常规”选项卡内列出了对 DHCP 服务器进行配置的选项及说明。在上面的列表框中，选择需要修改的选项，在下面就会列出相应的值。比如在上面的列表框中选择了 DNS 服务器，下面就会显示和 DNS 服务器对应的选项修改界面，修改后，单击最下面的“确定”按钮即可

完成修改,如图10-25所示。




图10-25　配置服务器选项

2)作用域选项的配置

在DHCP管理控制窗口的左侧,展开对象树,在"作用域"下的"作用域选项"上右击鼠标,选择弹出菜单的"配置选项",如图10-26所示。




图10-26　打开作用域选项

在打开的"作用域选项"窗口中,有"常规"和"高级"两个选项卡,"常规"选项卡用于配置作用域的常规选项,从上面的列表框中选择要修改的选项,下面即显示相应的修改界面。修改后,单击"确定"即完成修改,如图10-27所示。




图 10-27 修改作用域选项

### 10.2.3 DHCP 中继代理

路由器将多个物理网络连接起来，使多个物理网络实现了互联互通，但也隔离了各物理网络的广播包。而 DHCP 采用广播方式进行 IP 地址的分配，因此 DHCP 服务被限制在一个物理网络中，无法为其他物理网络中的客户机分配 IP。若要每个物理网络都使用 DHCP 进行网络信息的配置，需要为每个物理网络配置一台 DHCP 服务器，这样设备投资开销则太大。为了解决这个问题，可以通过 DHCP 中继代理的方法解决。如图 10-28 所示，路由器连接着两个物理网络：子网 A，IP 地址为 192.168.1.1-254/24；子网 B，IP 地址为 172.16.1.1-254/24。子网 A 中有一 DHCP 服务器，其 IP 为 192.168.1.200/24；子网 B 中有一 DHCP 中继代理，其 IP 为 172.16.1.200/24。子网 B 中的 DHCP 客户机通过广播方式发出 IP 分配请求，由于路由器阻隔了广播包，DHCP 服务器无法接收到这个广播包，子网

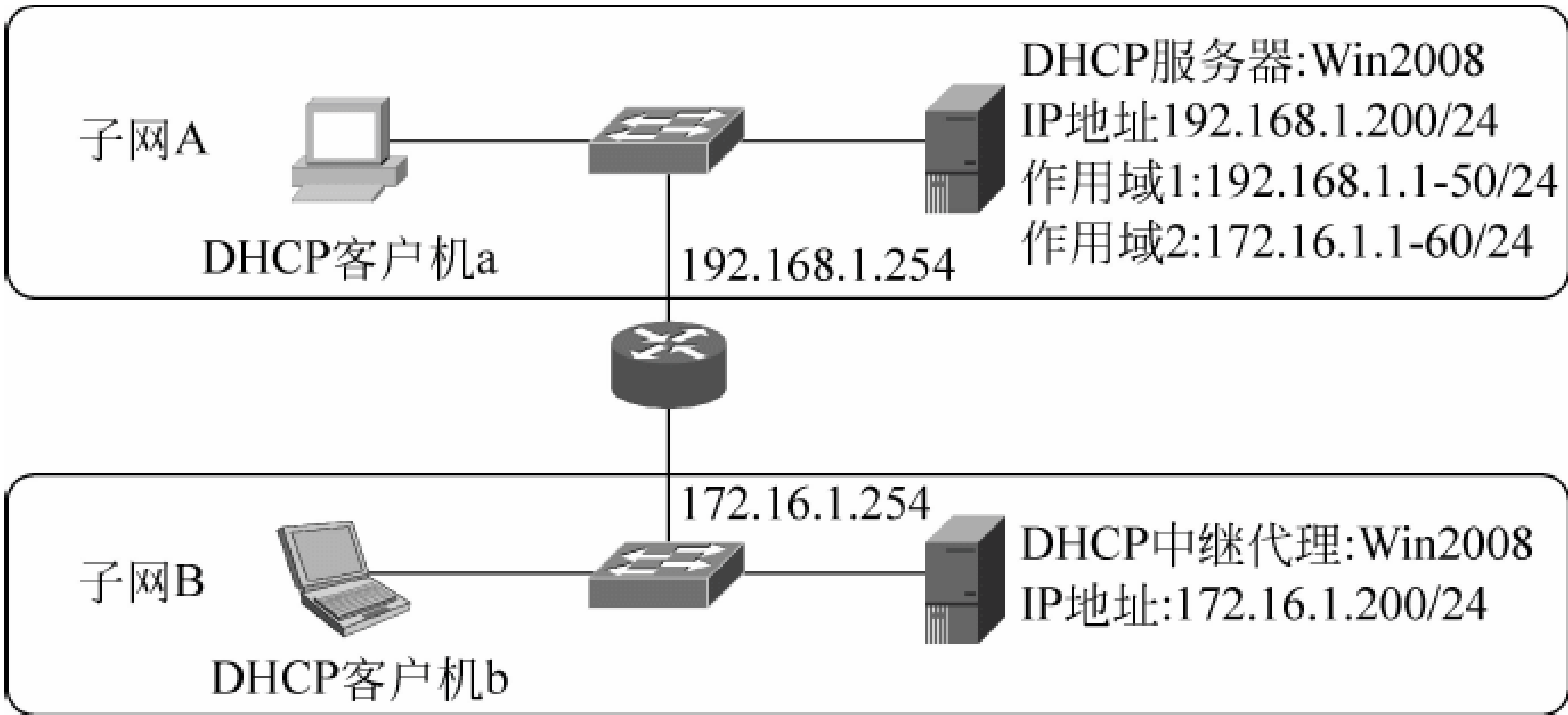



图 10-28 DHCP 中继代理的使用

B 中的客户机必须通过 DHCP 中继代理向 DHCP 服务器申请。信息的具体传递过程如下。

（1）子网 B 中的客户机通过广播方式向外发出 IP 分配请求 DHCPDISCOVER，由于路由器的作用广播包被限制在了子网范围内，无法到达 DHCP 服务器。子网 B 中的 DHCP 中继代理接收到这个信息后，以单播方式向 A 子网中的 DHCP 服务器转发了这个请求，由于是单播，信息通过路由器到达 DHCP 服务器。

（2）DHCP 服务器收到这个请求后，也以单播的方式把 DHCPOFFER 发送给 B 子网中的 DHCP 中继代理，中继代理又以广播方式向 B 子网中的所有主机广播这个信息。

（3）B 子网中的客户端收到这个广播包后，又广播了 DHCPREQUEST 信息，中继代理又以单播的方式转发给 A 子网中的 DHCP 服务器。

（4）A 子网中的 DHCP 服务器，以单播方式把 DHCPACK 发给了 B 子网中的中继代理，中继代理向 B 子网广播了这个信息。B 子网中的客户机收到这个信息。至此完成 IP 地址的申请与分配。

以这种方式每个子网还得有一台 DHCP 中继代理，依然造成巨大的浪费。好在现在的路由器都支持 DHCP 代理协议，可以由路由器来完成 DHCP 中继代理的工作，从而省掉了中继代理这台机器。

### 10.2.4　创建超级作用域

通常情况下，DHCP 服务器的作用域只能为客户端分配与它自身在同一网段的 IP 地址。而在实际应用中，当作用域所在子网的可用 IP 地址即将用尽，但网络中需要申请 IP 的主机却在不断增加；或者服务器接收来自不同子网的 IP 分配请求，这时可以使用多个作用域的地址空间进行 IP 地址的分配。超级作用域正好是解决这个问题的利器，超级作用域可以把多个不同作用域整合成为单个实体，为客户分配来自多个作用域的 IP 地址。下面介绍超级作用域的建立过程。

步骤 1：在 DHCP 管理控制窗口中，右击左侧的 IPv4，在弹出的菜单中选择“新建超级作用域”，如图 10-29 所示。

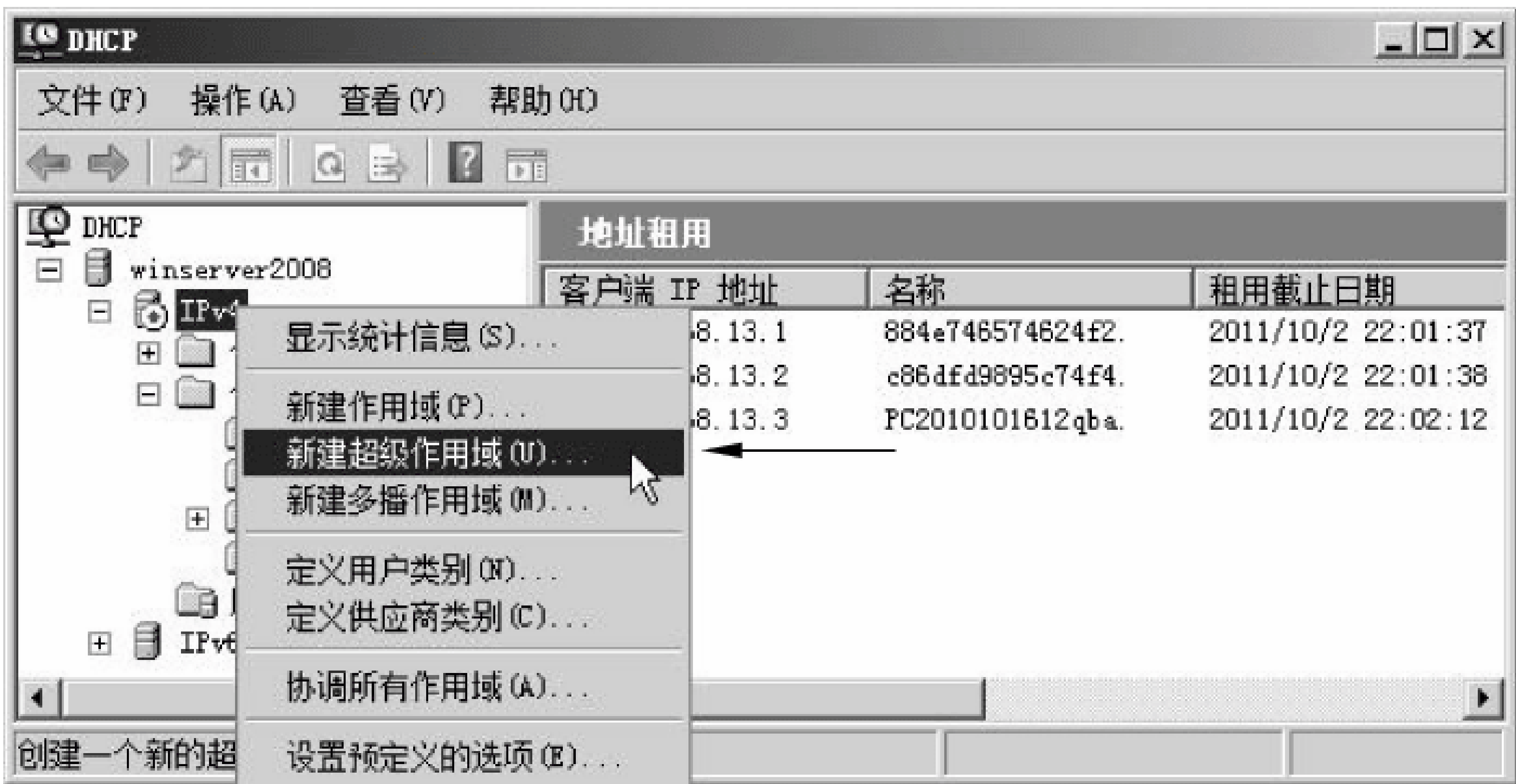



图 10-29　新建超级作用域

步骤 2：进入“新建超级作用域向导”的输入超级作用域名称步骤，在名称栏中输入超级作用域的名称，如图 10-30 所示。




图 10-30　输入超级作用域的名称

步骤 3：在向导的选择作用域窗口，可以选择已经建立的作用域作为超级作用域的成员。选择时，可以使用 Ctrl 或 Shift 键与鼠标协同选择多个作用域，如图 10-31 所示。




图 10-31　选择作用域

步骤 4：向导进入最后一步，显示超级作用域的信息，单击“完成”即可建立超级作用域。

建立超级作用域时可以将原来的作用域加入超级作用域，也可以先建立超级作用域，在超级作用域中建立的作用域自然就属于超级域；也可以先建作用域，单击鼠标右键选“添加到超级作用域”进行添加。

若要删除超级作用域,右击欲删除的“超级作用”,在快捷菜单中,选择“删除超级作用域”,单击确认对话框中的“确认”即可删除超级作用域。删除超级作用域不会影响原有作用域。

图 10-32 所示为 DHCP 服务器所在子网 192.168.13.0 的 IP 地址分配情况,图 10-33 为超级作用域下另一作用域 IP 分配情况,这说明超级作用域把 DHCP 服务器中的两个作用域整合成为了一个实体,用两个网段的地址空间为客户分配地址。




图 10-32　超级作域中第一个作用域的 IP 租用情况




图 10-33　超级作用域中第二个作用域 IP 租用情况

# 10.3　DHCP 客户机的配置与测试

配置完 DHCP 服务器以后,客户机只要设置为“自动获得 IP 地址”与“自动获得 DNS 服务器地址”即可自动获得 IP 地址。下面介绍客户机的配置过程。

Windows 2000/XP 下，依次选择“开始”→“控制面板”→“网络连接”→“本地连接”，右击选择“属性”，在“本地连接属性”窗口中选择“Internet 协议(TCP/IP)”选项，单击“属性”，打开如图 10-34 所示窗口，选择“自动获得 IP 地址”和“自动获得 DNS 服务器地址”，单击“确定”按钮。依次选择“开始”→“运行”，输入“cmd”，打开命令行窗口，输入 ipconfig /all 即可查看网络信息；输入 ipconfig /release 释放获得的 IP 地址，输入 ipconfig /renew 重新获得 IP 地址。

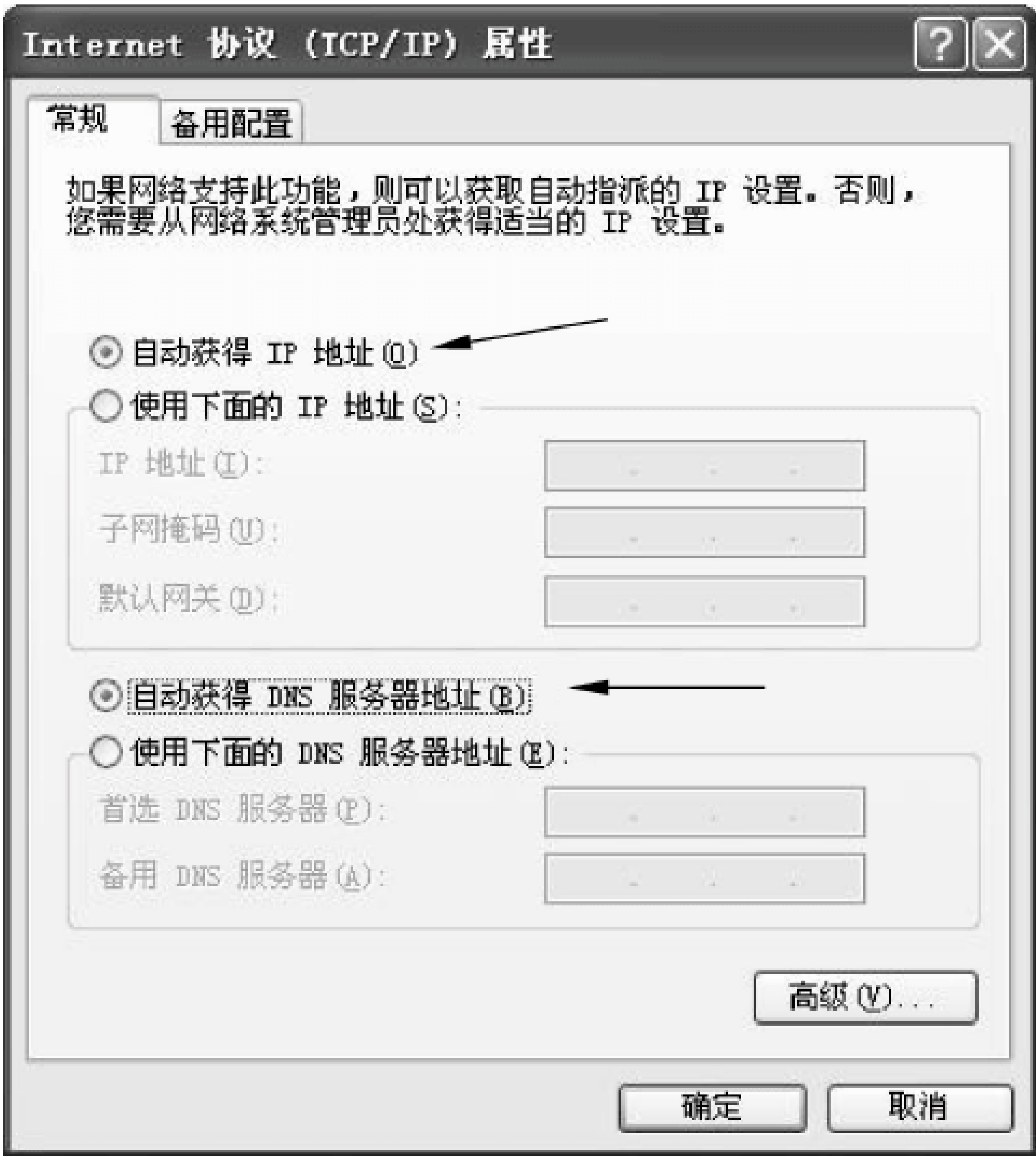



图 10-34　Internet 协议(TCP/IP)属性

# 实验 15　DHCP 服务器的配置

**1. 实验目标**

(1) 掌握 DHCP 的工作原理。

(2) 掌握 Windows Server 2008 下 DHCP 服务器的配置方法。

**2. 实验准备**

一台安装了 Windows Server 2008 的服务器，一台客户机；或者一台安装了虚拟机的性能较好的计算机。

**3. 实验内容**

(1) DHCP 服务器的安装。

(2) 在 DHCP 服务器中创建作用域，具体参数如下。

IP 地址段为：192.168.1.1～192.168.1.200

子网掩码为：255.255.255.0

网关地址为：192.168.1.254

域名服务器为：192.168.0.1

子网所属的域名为：lnpc.cn

默认的租期为：1 天

排除地址为：192.168.1.50～192.168.1.55

为一客户机保留 IP 为：192.168.1.100

(3) 在 Windows 客户机上测试 DHCP 服务器的工作是否正常。

# 思考与练习

**一、填空题**

1. DHCP 是动态主机配置协议，其英文全称是________________。

2. 分配 IP 地址的方法有两种，一种是静态分配 IP 地址，另一种是________。

3. 配置 DHCP 服务器时，为某一客户机保留特定的 IP 是根据________来判断客户身份的。

4. DHCP 进行网络配置时，配置网络参数包括：IP 地址、子网掩码、网关地址、________地址等网络属性。

**二、选择题**

1. TCP/IP 中，(　　)协议是用来进行 IP 地址自动分配的。

　A. ARP　　B. NFS　　C. DHCP　　D. DDNS

2. DHCP 可以分为两个部分：一个是客户端，一个是(　　)。

　A. 服务器端　　B. 客户机　　C. 服务器　　D. 服务端

3. DHCP 租用 IP 地址的过程有：IP 租用请求、IP 地址租用提供、IP 租用选择和(　　)。

　A. IP 租用确认　　B. IP 的测试　　C. IP 的分配　　D. IP 的传输

4. DHCP 是基于(　　)模式的，它允许 DHCP 服务器向客户端动态分配 IP 地址和配置信息。

　A. C/S　　B. www　　C. 域　　D. 工作组

5. 查看系统的 MAC 地址，可以使用下面的命令(　　)。

　A. ipconfig /all　　B. ipconfig /release

　C. ipconfig /renew　　B. ping

**三、问答题**

1. 简述使用 DHCP 进行网络配置的好处与场合。

2. 简述 DHCP 的工作原理。

3. 如何设置 DHCP 客户机？

4. 什么是 DHCP 的“特定 IP 地址保留”功能？它与排除地址有什么不同？

第 11 章

# Web 服务器的配置与管理

## 11.1 Web 与 Web 服务器

### 11.1.1 Web 概述

Internet 是当今规模最大、覆盖最广、用户最多、资源最丰富的计算机网络，Internet 采用 TCP/IP 协议进行通信，把各国、各地区、各部门连接在一起，整个 Internet 成为一个没有国界，没有空间限制的网络。从其诞生之日起应用越来越广泛，用户越来越多，影响也越来越深远。

Internet 上的网络信息资源信息量大，类型丰富。接入 Internet 的服务器每年都在以几何级数的速度增长，网上数据除了文本形式外，还有图片、音频、视频等多种类型，采用超文本或超媒体技术，把网络上的这些信息连接起来，形成一张巨大的知识网。网络上的信息更新变化速度非常快，时效性很强。每天都有新的内容被发布，旧的过时的内容被淘汰。网络上的信息同时也是分散无序的。

Web 是 Internet 中分布最为广泛的一种资源，它其实是 World Wide Web 的简称，从这个名字可以看出其广泛性，现在 WWW 俨然成了网络的代名词。Web 的广泛应用是和它的优点分不开的，概括起来 Web 具有下列特点。

(1) Web 是图形化的和易于导航的。Web 非常流行的一个很重要的原因就在于它可以在页面上同时显示形式多样的文本、图形和多媒体信息。同时，Web 是非常易于导航的，只需要从一个链接跳到另一个链接，就可以在各页各站点之间进行浏览了。

(2) Web 具有交互性。网页中大量地使用了超链接，通过超链接用户的浏览顺序和所到站点完全由他自己决定。另外网页中大量地使用了表单，通过表单可以从服务器获得动态信息。用户通过填写表单可以向服务器提交请求，服务器可以根据用户的请求返回相应信息。

(3) Web 具有动态性。随着技术的进步，越来越多的 Web 发布系统开始支持动态网页的发布，把数据库中的信息以 Web 网页的方式发布出来，实时更新，也加强了和用户的交互性。

(4) Web 具有平台无关性。不管是什么平台：Windows 平台、Linux 平台、UNIX 平台、Macintosh 还是别的什么平台我们都可以访问 WWW。对 WWW 的访问是通过一种叫

做浏览器(Browser)的软件实现的。如开源的 Firefox、Microsoft 的 Internet Explorer 等。

### 11.1.2　常用 Web 服务器介绍

WWW 采用的是浏览器/服务器结构,其作用是整理和储存各种 WWW 资源,并响应客户端软件的请求,把客户所需的资源传送给客户机。Web 服务器在整个 Internet 网络中占有非常重要的地位,下面介绍几个常用的 Web 服务器。

**1. Apache 服务器**

Apache 是一种开源的 Web 服务器软件,它源于 NCSA httpd 服务器,当 NCSA WWW 服务器项目停止后,那些使用 NCSA WWW 服务器的人们开始交换用于此服务器的补丁,这也是 Apache 名称的由来(A patchy Server,一个充满补丁的服务器)。Apache 是世界上用得最多的 Web 服务器,市场占有率达 60%左右。Apache 成功的原因在于它的源代码开放、有一支开放的开发队伍、支持跨平台的应用(可以运行在几乎所有的 UNIX、Windows、Linux 系统平台上)以及它的可移植性等方面。

**2. IIS 服务器**

Microsoft 的 Web 服务器产品为 Internet Information Service(IIS),IIS 是允许在公共 Intranet 或 Internet 上发布信息的 Web 服务器。IIS 是目前最流行的 Web 服务器产品之一,据统计 2011 年其市场占有率为 18.83%,居第二的位置,很多著名的网站都是建立在 IIS 平台上的。IIS 提供了一个图形界面的管理工具,称为 Internet 服务管理器,可用于监视配置和控制 Internet 服务。

IIS 是一种 Web 服务组件,其中包括 Web 服务器、FTP 服务器、NNTP 服务器和 SMTP 服务器,分别用于网页浏览、文件传输、新闻服务和邮件发送等方面,它使得在网络(包括互联网和局域网)上发布信息成为一件很容易的事。它提供 ISAPI(Intranet Server API)作为扩展 Web 服务器功能的编程接口;同时,它还提供一个 Internet 数据库连接器,可以实现对数据库的查询和更新。

**3. Nginx**

Nginx("engine x")是一个高性能的 HTTP 和反向代理服务器,也是一个 IMAP/POP3/SMTP 代理服务器。Nginx 是由 Igor Sysoev 为俄罗斯访问量第二的 Rambler.ru 站点开发的,第一个公开版本 0.1.0 发布于 2004 年 10 月 4 日。其将源代码以类 BSD 许可证的形式发布,因它的稳定性、丰富的功能集、示例配置文件和低系统资源的消耗而闻名。2011 年 6 月 1 日,Nginx 1.0.4 发布。2011 年统计它的市场占有率为 7.5%,居第三位。

Nginx 是一个很牛的高性能 Web 和反向代理服务器,Nginx 以事件驱动的方式编写,所以有非常好的性能,在高连接并发的情况下,Nginx 是 Apache 服务器不错的替代品;在反向代理、负载均衡方面 Nginx 也有不俗的表现;Nginx 也是一个非常优秀的邮件代理服务器(最早开发这个产品的目的之一也是作为邮件代理服务器)。

**4. Lighttpd**

Lighttpd 是一个德国人领导的开源软件,其根本目的是提供一个专门针对高性能网站,安全、快速、兼容性好并且灵活的 Web Server 环境。具有非常低的内存开销,CPU 占用率低,效能好,以及丰富的模块等特点。Lighttpd 是众多 Open Source 轻量级 Web Server 中较为优秀的一个。支持 FastCGI、CGI、Auth、输出压缩(Output Compress,OC)、URL 重写, Alias 等重要功能,而 Apache 之所以流行,很大程度也是因为功能丰富,在 Lighttpd 上很多功能都有相应的实现。

**5. Tomcat**

Tomcat 是一个开放源代码,运行 Servlet 和 JSP Web 应用软件的基于 Java 的 Web 应用软件容器。Tomcat Server 是根据 Servlet 和 JSP 规范执行的,因此我们就可以说 Tomcat Server 也实行了 Apache-Jakarta 规范且比绝大多数商业应用软件服务器要好。

**6. Resin**

Resin 是 CAUCHO 公司的产品,是一个非常流行的支持 Servlets 和 JSP 的引擎,速度非常快。Resin 本身包含了一个支持 HTTP/1.1 的 Web 服务器。虽然它可以显示动态内容,但是它显示静态内容的能力也非常强,速度直逼 Apache Server。许多站点都是使用该 Web 服务器构建的。

Resin 也可以和许多其他的 Web 服务器一起工作,比如 Apache Server、IIS 等。Resin 支持 Servlets 2.3 标准和 JSP 1.2 标准。熟悉 ASP 和 PHP 的用户可以发现用 Resin 来进行 JSP 编程是件很容易的事情。

Resin 支持负载均衡(Load Balancing),可以增加 Web 站点的可靠性。方法是增加服务器的数量。比如一台 Server 的错误率是 1%的话,那么支持负载均衡的两个 Resin 服务器就可以使错误率降到 0.01%。

## 11.2 IIS 服务器安装与配置

### 11.2.1 IIS 服务器的安装

步骤 1:依次选择“开始”→“管理工具”→“服务器管理器”,打开服务器管理器,选择窗口左侧“角色”,单击右侧“添加角色”,如图 11-1 所示。

步骤 2:进入添加角色向导的“开始之前”步骤,单击“下一步”按钮。

步骤 3:进入添加角色向导的“服务器角色”步骤,单击弹出窗口“添加角色向导”中的“添加必要的功能”。

步骤 4:进入添加角色向导的“服务器角色”步骤,单击“Web 服务器(IIS)”复选框,如图 11-2 所示。单击“下一步”按钮。

步骤 5:进入添加角色向导的“Web 服务器(IIS)”步骤,单击“下一步”按钮。

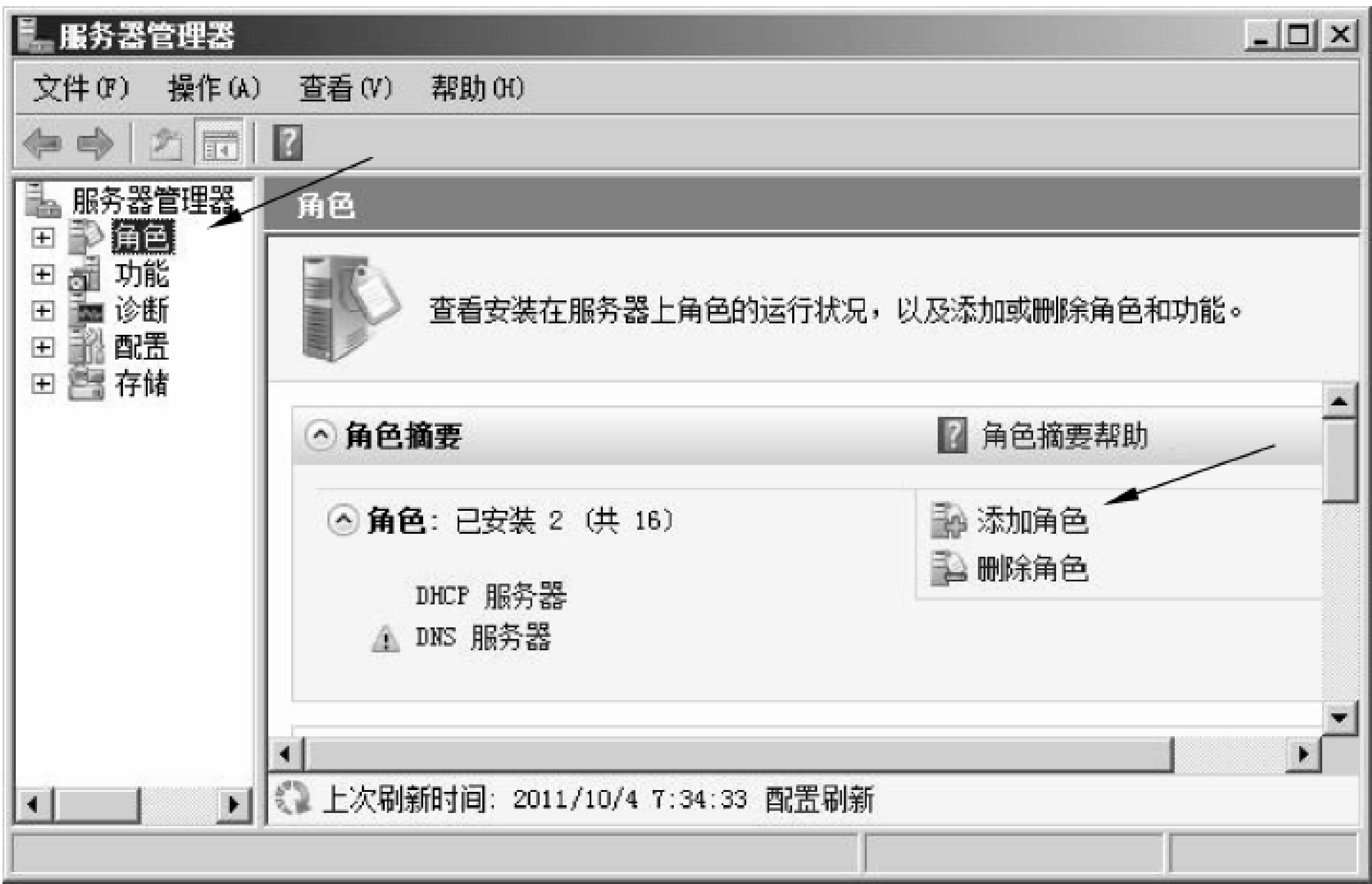



图 11-1　添加 IIS 角色




图 11-2　选择安装 Web 服务器

步骤 6：进入添加角色向导的“角色服务”步骤，在窗口右侧，选中“常见 HTTP 功能”下的所有选择，单击“下一步”按钮，如图 11-3 所示。

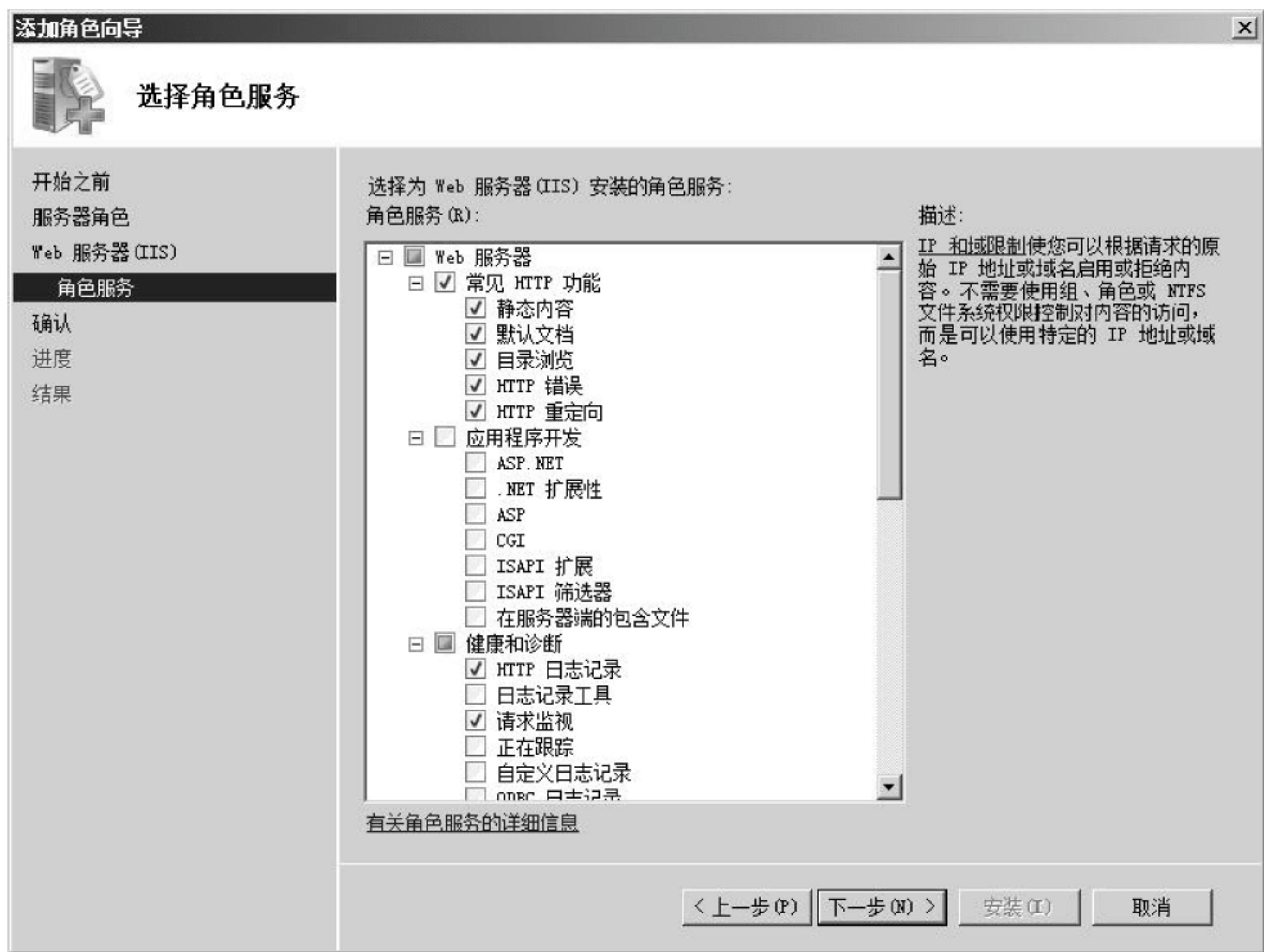



图 11-3　选择将要安装的角色服务

步骤 7：进入添加角色向导的“确认”步骤，单击“安装”按钮，开始安装。

步骤 8：进入添加角色向导的“结果”步骤，单击“关闭”结束安装过程。

步骤 9：测试 IIS 是否安装成功。在客户机上打开 IE，在 IE 地址栏中输入 IIS 服务器的 IP 地址 http://192.168.13.200，如果一切正常的话，可见到如下的欢迎界面，如图 11-4 所示。

## 11.2.2　IIS 服务器的基本设置

IIS 服务器安装完成以后，可以通过以下方式进行 Web 服务器的配置。

方法一：依次选择“开始”→“管理工具”→“Internet 信息服务(IIS)管理器”，打开 Internet 信息服务(IIS)管理器。

方法二：依次选择“开始”→“管理工具”→“服务器管理器”。打开服务器管理器，在窗口的左侧依次展开“角色”→“Web 服务器”→“Internet 信息服务(IIS)管理器”，窗口的右侧就会呈现出管理界面。

方法三：依次打开“开始”→“运行”，在运行对话框中输入 inetmgr，单击“确定”，也可打开 Internet 信息服务(IIS)管理器。




图 11-4　IIS 的默认欢迎界面

### 1. 启动/停止 IIS 服务器

常见的启动或停止 IIS 服务的方式有三种。

(1) 在“Internet 信息服务(IIS)管理器”左边窗格中选择服务器的名称,在右边窗格中有“重新启动”、“启动”、“停止”按钮,单击即可执行相应动作,如图 11-5 所示。




图 11-5　在管理器窗口中启动/停止 IIS 服务

（2）依次选择“开始”→“管理工具”→“服务”，打开服务窗口，选择 World Wide Web Publishing Service 服务项，单击图中椭圆圈住的按钮，或右击服务的名称，选择“启动”、“停止”、“暂停”、“重新启动”等选项也能执行相应的动作，如图 11-6 所示。




图 11-6　在服务窗口中启动/停止 IIS 服务

（3）在“Internet 信息服务(IIS)管理器”左边窗格中右击服务器名称，弹出菜单中有“启动”、“停止”等菜单项，选择即可执行相应的功能，如图 11-7 所示。




图 11-7　从服务器名称上启动/停止 IIS 服务

**2. 网站 IP 地址的绑定**

每个 Web 服务器都有一个或多个 IP 地址，某一网站到底使用哪个 IP 地址需要设置一下。打开 Internet 信息服务(IIS)管理器，在左侧依次展开“服务器名称”→“网站”→Default Web Site，在窗口中间位置选“IPv4 地址和域限制”，在窗口右侧单击“绑定”。打开如图 11-8 所示的网站绑定对话框，在该对话框中，选择列表框中的主机名为空，IP 地址为“*”的网站，然后单击“编辑”。




图 11-8　网站 IP 地址的绑定

打开图 11-9 所示的“编辑网站绑定”对话框，在 IP 地址栏，单击三角符号选择准备绑定的本服务器的 IP 地址，在主机名文本框中输入主机名。单击“编辑网站绑定”对话框的“确定”按钮，再单击“网站绑定”对话框中的“关闭”按钮。

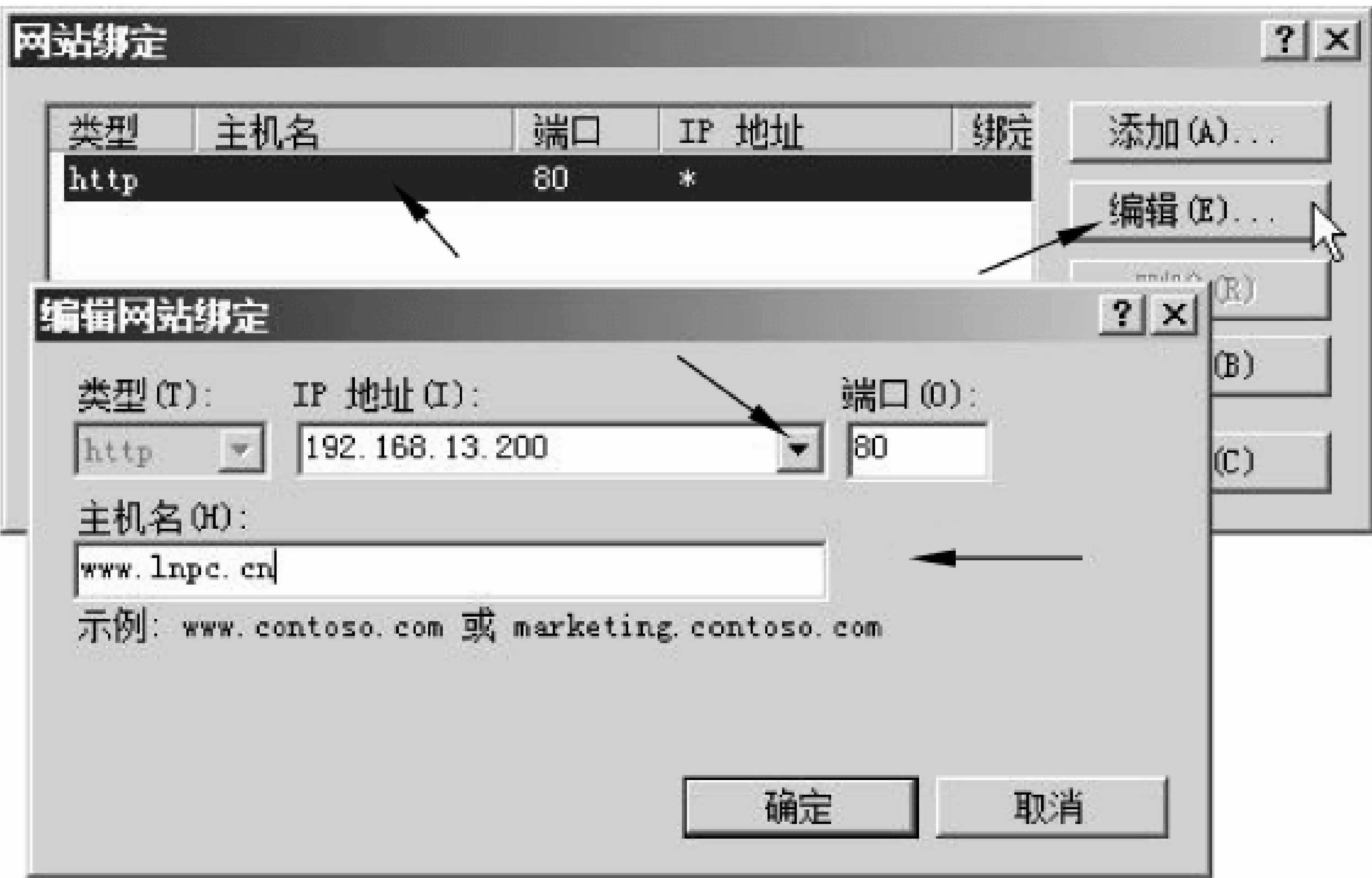



图 11-9　“编辑网站绑定”对话框

### 3. 网页存储位置的设置

在如图 11-10 所示的“Internet 信息服务(IIS)管理器”中选中“网站”下的 Default Web Site，在右侧的“操作”窗格中选“基本设置”选项。

打开“编辑网站”对话框，如果要重新设置网站的物理存储路径，单击“物理路径”文本框右侧的“..”按钮，指定想设置为网页存储位置的目录，单击“确定”完成设置。




图 11-10　设置网站的网页存储位置

### 4. 设置网站的默认主页

选择“Internet 信息服务(IIS)管理器”左边窗格中“网站”下的 Default Web Site,再双击中间窗格中的“默认文档”,中间窗格中就会显示当前网站的默认主页。单击右边窗格中的“添加”添加一个网站的默认主页;选择中部窗格中的文档,单击右边窗格中的“删除”,删除一个默认主页;选择中部窗格中的一个文档,单击右边的“上移”、“下移”,可以改变文档在网站中排列顺序,在上面的文档先被搜索到,如图 11-11 所示。




图 11-11　网站默认主页的设置

### 11.2.3　用 IIS 发网页

**1. 使用默认网站发布网页**

一般情况下，没有什么特殊要求使用系统默认的网站就可以发布网页。把网页文件复制到 C:\inetpub\wwwroot 目录下，把网站主页改名为 Default.htm。建议初学者先尝试使用默认网站发布网页。

**2. 新建网站**

若不使用默认的网站发布网页，则需要新建网站。下面我们一起来新建一个网站，并发布默认网页 myfirst.html。

步骤 1：打开“Internet 信息服务(IIS)管理器”，在左边窗格中右击“网站”，选择弹出菜单中的“添加网站”，如图 11-12 所示。

步骤 2：打开“添加网站”窗口，在“网站名称”栏输入网站名称，单击“物理路径”右侧的“..”按钮，选择存放网页的物理路径。在“IP 地址”组合框中，选择服务器的 IP 地址，单击“确认”按钮，如图 11-13 所示。




图 11-12　选择弹出菜单“添加网站”

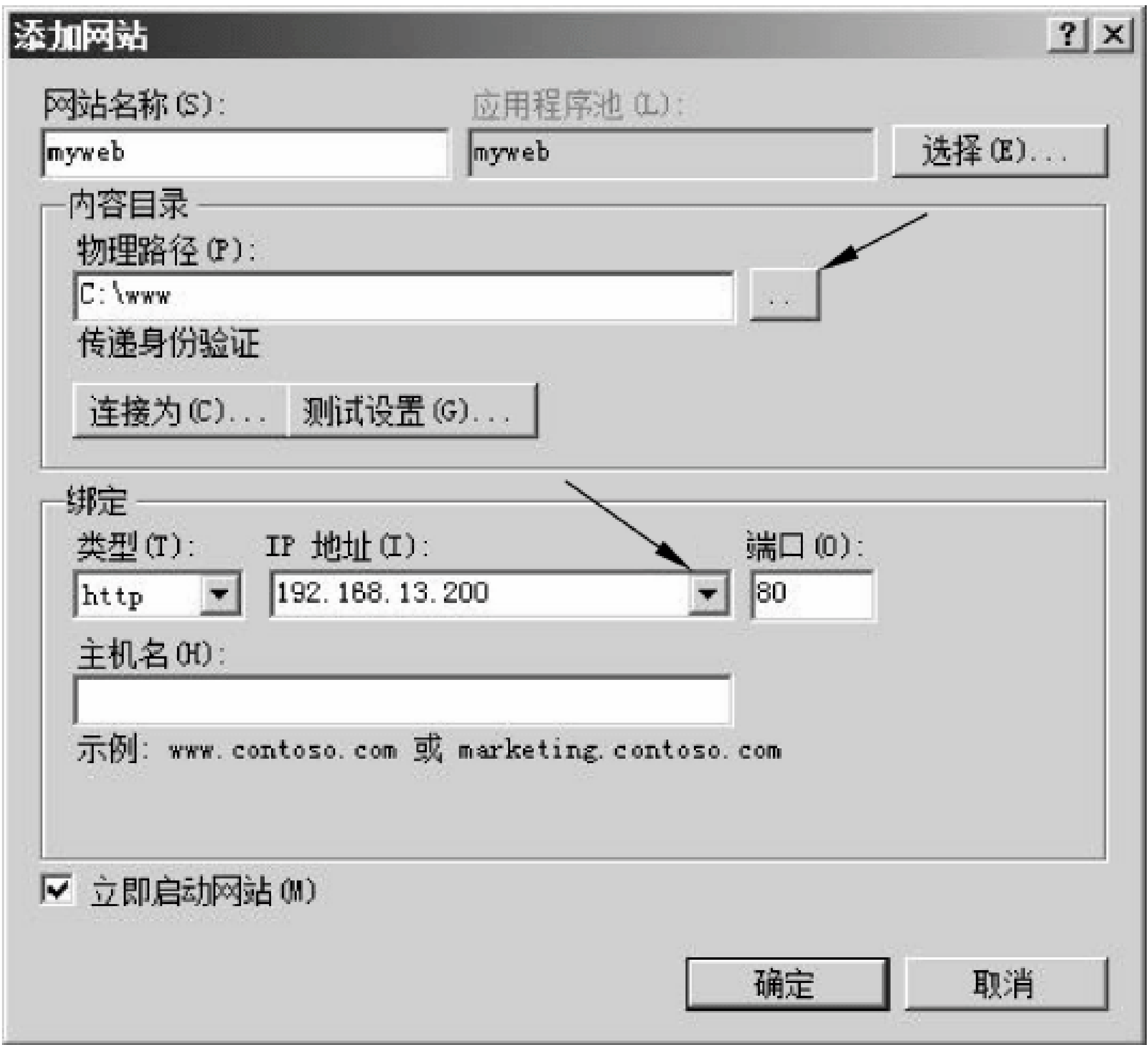



图 11-13　“添加网站”窗口

步骤 3：停止默认网站。因为默认网站绑定了 IIS 服务器的 IP 地址，新建的网站也绑定了 IIS 服务器的 IP 地址，应停止默认网站。方法是在“Internet 信息服务(IIS)管理器”窗口中，单击 Default Web Site，在右侧“操作”窗格中，单击“停止”按钮，停止默认网站，如图 11-14 所示。

步骤 4：添加“默认文档”。在“Internet 信息服务(IIS)管理器”窗口，单击左侧窗格中的 myweb 网站，再双击中部窗格中的“默认文档”，打开图 11-15 所示的界面，右击“操作”窗格中的“添加”，在弹出窗口中输入网站首页文档名 myfirst.html。



图 11-14　停止默认网站



图 11-15　设置默认文档

步骤 5：在客户端打开浏览器，输入 IIS 服务器的 IP 地址即可浏览发布的网页。

### 11.2.4　建立虚拟目录

上一节发布网页时，我们把网页放在了系统默认的 C:\inetpub\wwwroot 目录下，或者其他目录，如 C:\www，这些物理目录叫做主目录。主目录对应着网站的根目录，在主目录下的网页都可以发布出去，然而，有时需要发布主目录之外的其他目录下的网页，使它成为

网站的有机组成部分，这时怎么办呢？要发布主目录之外的其他目录下的网页，可以使用虚拟目录技术。

使用虚拟目录具有以下优点。

（1）提高 Web 服务器的安全性。使用虚拟目录，把网页放到了主目录之外，网站用户并不知道网页文件真正存放在什么位置，不能修改/删除网页文件。

（2）提高网站建设的灵活性。比如网站下有一目录为 video，它对应的物理路径为 D:\video 目录，由于视频文件太大，服务器的 D 盘空间不够，把它转到别的服务器或专用存储设备，这时只需要把网站下的 video 目录和物理目录的对应关系改变一下就可以了，用户看到的还是 video 目录，网站逻辑关系并未改变。

（3）均衡了服务器的负载。由于网络资源存放在了不同的物理设备上，当网站负载较大时，不会因为 I/O 瓶颈使网站性能下降。

下面用一个实际例子说明虚拟目录的建立。

步骤 1：在 C:\盘下，建立文件夹 video，并在其下建立文件 default. htm，文件内容是“＜H1＞这里是视频点播，在 c:\video 下＜/H1＞”。

步骤 2：在“Internet 信息服务(IIS)管理器”中右击网站下的 Default Web Site，从弹出菜单中选择“添加虚拟目录”。

步骤 3：弹出对话框“添加虚拟目录”，在别名文本框中，输入 video，在物理路径中输入 C:\video，或单击“..”按钮，选择“C:\video”。单击“确定”按钮。

打开浏览器，输入 http://192. 168. 13. 200/video/即可浏览虚拟目录下的网页了，如图 11-16 所示。




图 11-16　虚拟目录的建立

## 11.2.5 HTTP 重定向

如果网站正在建设中,内容还未建设完成,这时就需要把建设中的网站重定向到另外一个网站。客户浏览建设中的网站时打开的是另外一个网站。默认情况下,没有安装重定向服务,需要安装重定向服务。

**1. 安装 HTTP 重定向服务**

步骤 1:打开“服务器管理器”窗口,展开左侧“角色”选项,单击“Web 服务器”,在窗口右边选择“添加角色服务”,如图 11-17 所示。




图 11-17 添加角色服务

步骤 2:在打开的“添加角色服务”窗口中,如图 11-18 所示,选择“HTTP 重定向”,单击“下一步”按钮。

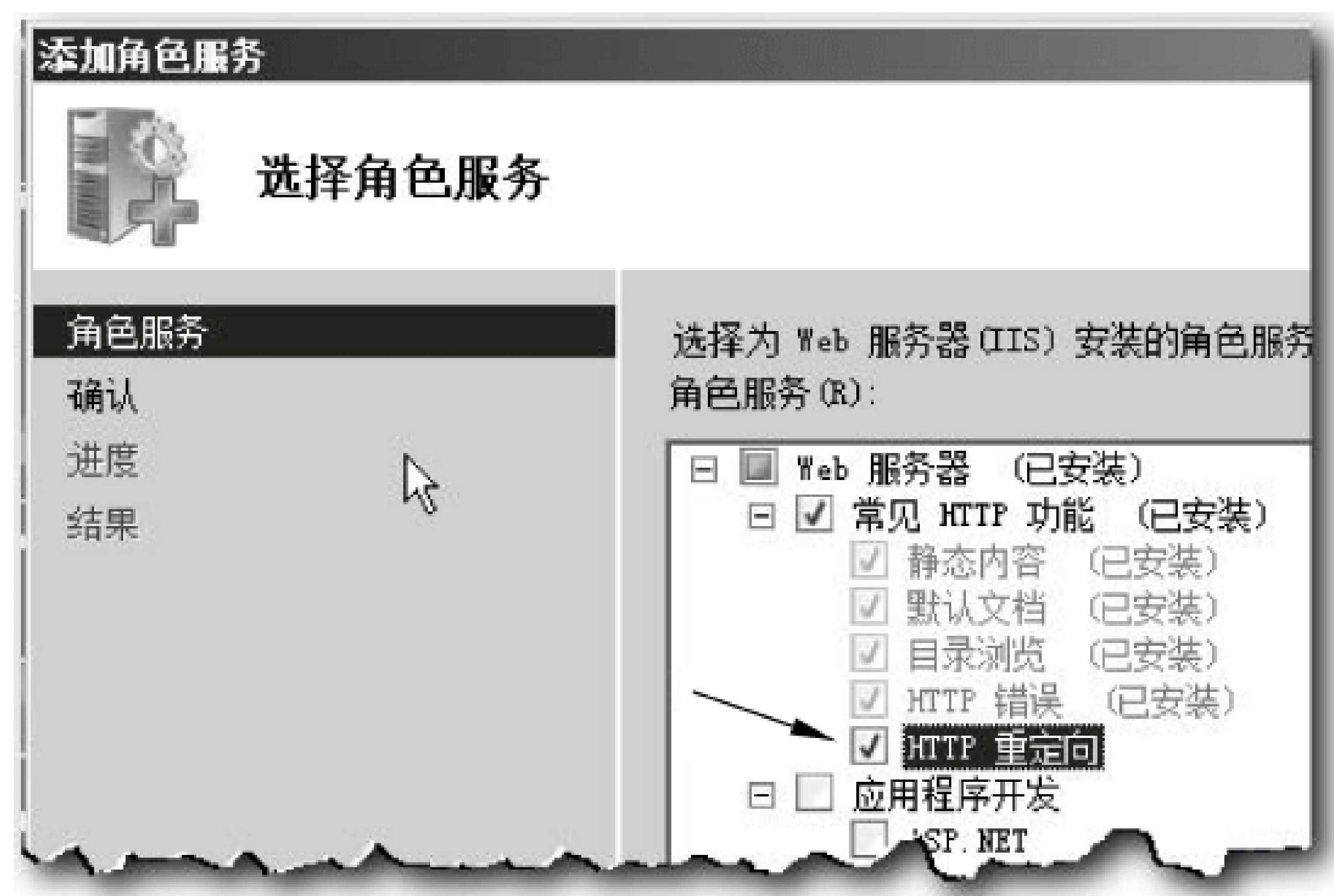



图 11-18 选中 HTTP 重定向服务

步骤 3:进入向导的“确认”步骤,单击“安装”,开始安装。

步骤 4:进入向导的“结果”步骤,单击“关闭”,完成安装。

### 2. 设置重定向

现在以上面建的两个网站为例来讲解 HTTP 重定向的设置方法。默认网站的访问地址是 http://192.168.13.200，myweb 网站的访问地址是 http://192.168.13.200:8080。

(1) 更改 myweb 网站的端口

因为 myweb 和默认网站运行在同一 IIS 服务器内，需要把它绑定在不同的端口上它们才能同时运行。

步骤 1：在“Internet 信息服务(IIS)管理器”左侧窗格中右击 myweb，选择弹出菜单中的“编辑绑定”，如图 11-19 所示。




图 11-19　设置 myweb 网站的端口

步骤 2：在打开的“网站绑定”对话框中，选择其中的 192.168.13.200 网站，单击“编辑”按钮。

步骤 3：在打开的“编辑网站绑定”对话框中，把端口由原来的 80 改为 8080。单击“确定”按钮。

(2) 设置 myweb 重定向

步骤 1：在“Internet 信息服务(IIS)管理器”左侧窗格中单击 myweb 网站，中间窗格显示任务选项。

步骤 2：在窗口的中间窗格中，双击“HTTP 重定向”。

步骤 3：窗口改变为如图 11-20 所示，选中“将请求重定向到此目标”，在文本框中输入 http://192.168.13.200，在重定向行为中选中“将所有请求重定向到确切的目标(而不是相对于目标)”。单击“操作”窗格中的“应用”。




图 11-20　设置 myweb 网站的重定向

（3）打开浏览器，输入 myweb 的网址 http://192.168.13.200:8080，结果显示的是默认网址。说明 myweb 的网站（http://192.168.13.200:8080）已经重定向到了默认网址 http://192.168.13.200:80。

# 11.3　多网站实现技术

正如我们前面所讲解的那样，如果在一个服务器同时运行两个或两个以上的网站时，会产生冲突，如何消除冲突，在一台网络服务器中运营多个网站呢？要唯一地标识一个网站可以通过三种途径：IP 地址、端口和主机标识名。因此，可以通过这三种途径实现在一台服务器上运营多个网站。

## 11.3.1　使用不同 IP 地址架设不同网站

一般虚拟主机都使用多个 IP 地址，以确保不同的域名使用不同的 IP 地址。在一个服务器上使用多个 IP 地址，有两种方式：一种是服务器中有多块网卡，一个网卡绑定一个 IP 地址；另外一种方法是服务器只有一块网卡，这块网卡绑定多个 IP 地址。因路由器等网络设备端口比较紧张，一般服务器采用安装一个高性能网卡，绑定多个 IP 地址的方式。Windows 操作系统支持一块网卡绑定多个 IP 地址。下面介绍不同 IP 地址运营不同网站的技术。

（1）服务器一块网卡绑定多个 IP 地址。

步骤 1：依次选择“开始”→“控制面板”→“网络和共享中心”→“管理网络连接”，在打开

的“网络连接窗口”中双击“本地连接”，打开“本地连接状态”窗口，单击“属性”按钮。

步骤 2：打开“本地连接属性”窗口，选择“Internet 协议版本 4(TCP/IPv4)”，然后，单击“属性”按钮。

步骤 3：打开“Internet 协议版本 4(TCP/IPv4)属性”窗口，单击“高级”按钮。

步骤 4：打开“高级 TCP/IP 设置”窗口，单击“添加”按钮。

步骤 5：打开“TCP/IP 地址”对话框，输入新绑定的 IP 地址。单击“添加”按钮。

步骤 6：依次单击“确定”或“关闭”按钮，关闭各窗口，这时服务器就绑定了两个 IP 地址 192.168.13.200 和 192.168.13.198，如图 11-21 所示。

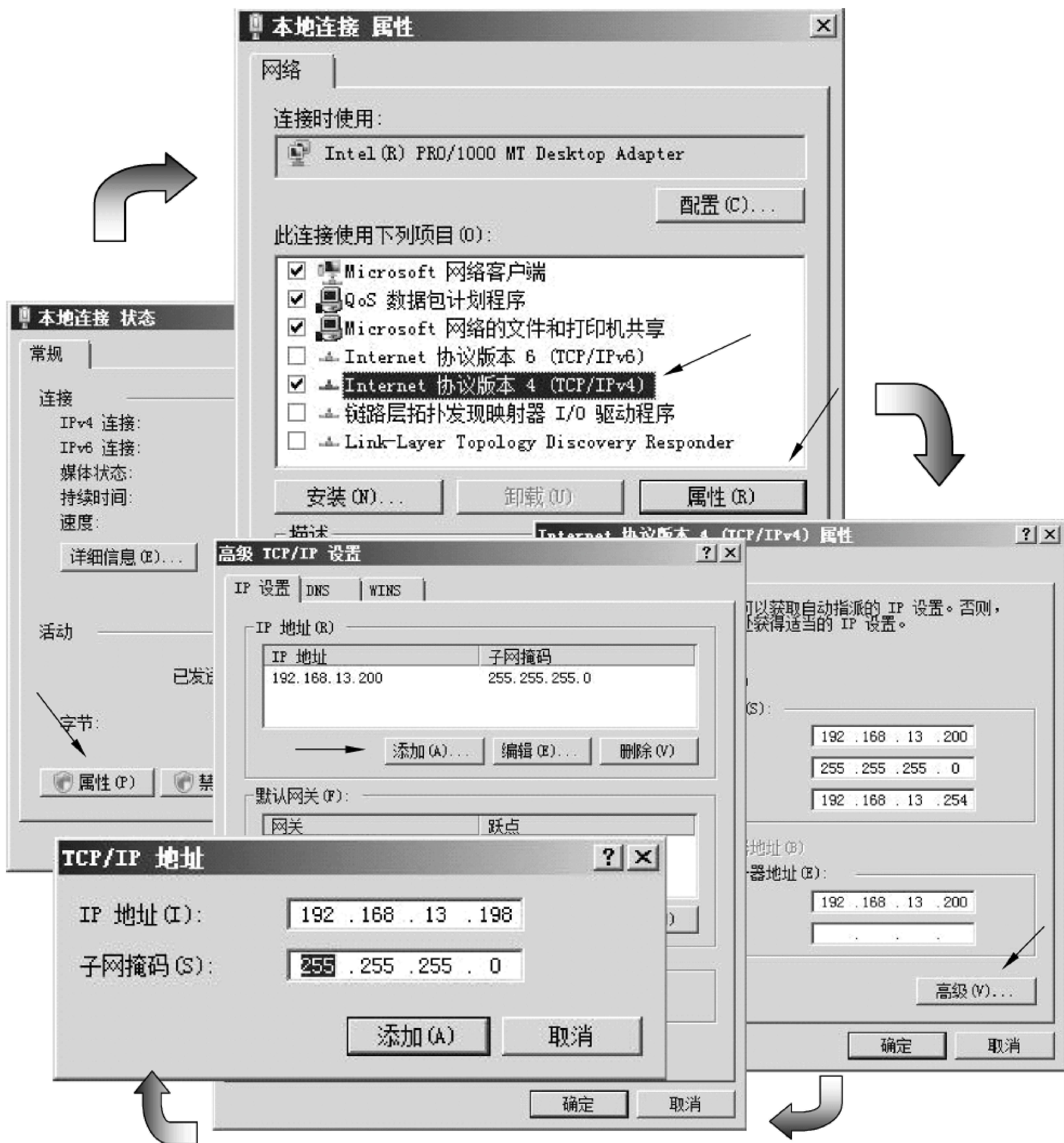



图 11-21　网卡绑定多个 IP 地址

（2）参照第 9 章，为域名添加两条记录：www.lnpc.cn 对应 IP 为 192.168.13.200，support.lnpc.cn 对应 IP 为 192.168.13.198，如图 11-22 所示。

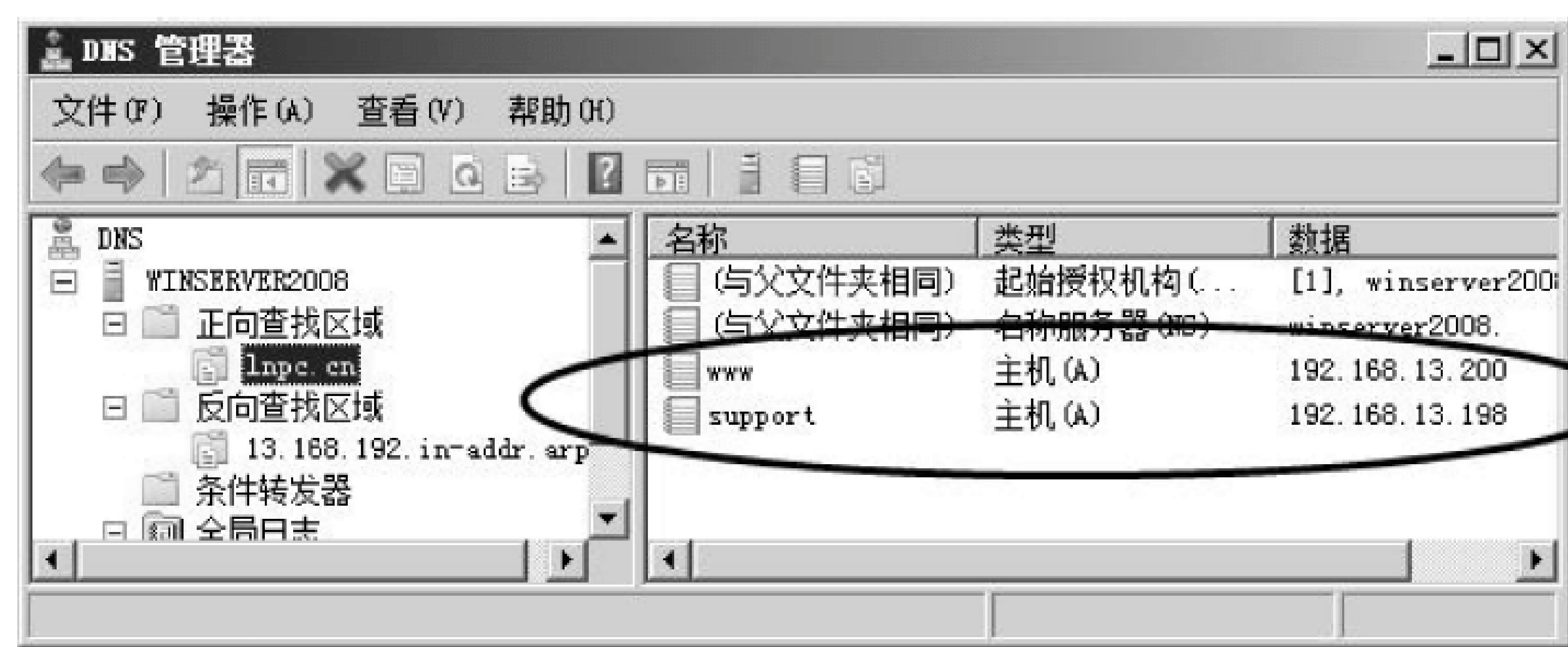



图 11-22　为域名添加记录

（3）为不同网站绑定不同的 IP 地址。参照 11.2.2 节内容，把 Default Web Site 网站绑定到 192.168.13.200，80 号端口；把 support 网站绑定到 192.168.13.198，80 号端口，如图 11-23 所示。




图 11-23　为不同的网站绑定不同的 IP 地址

（4）测试不同的网站

打开浏览器，分别输入 www.lnpc.cn 和 support.lnpc.cn，可以看到浏览的网页分别来自于不同的网站。

## 11.3.2 不同端口运营不同网站

上面的方法是比较传统的主机运营方式。随着网络的发展，IPv4 的地址越来越紧张了。为了减少 IP 地址的占用，一台服务器安装一块网卡，设置一个 IP 地址，但使用不同的端口，实现多网站运营。下面介绍设置方法。

现在我们假定 www.lnpc.cn 网站占用 192.168.13.200 的 80 端口，support.lnpc.cn 占用 192.168.13.200 的 8080 端口。

步骤 1：建立网页。

在 C:\inetpub\wwwroot\目录下建立 default.htm 文件，其内容是"<h1>这是 WWW 网站，端口是 80</h1>"；在 C:\support 目录下建立 default.htm 文件，其内容是"<h1>这是 support 网站，端口是 8080</h1>"

步骤 2：绑定 IP 地址和端口。

参照 11.2.2 小节内容，把 Default Web Site 网站绑定到 192.168.13.200，80 号端口；把 support 网站绑定到 192.168.13.200，8080 号端口，如图 11-24 所示。




图 11-24 为网站绑定 IP 地址和端口

步骤 3：测试不同端口上的不同网站，如图 11-25 所示。




图 11-25　不同端口运营不同网站

### 11.3.3　根据主机头架设不同网站

使用不同端口绑定不同网站，虽然实现了在一个服务器上运营多个网站，但给网站的用户带来了不必要的麻烦：必须记住网站的端口号。在以出租服务器空间营利的商业网站采用不同域名来标识不同的网站的方法，这种方法必须有 DNS 服务器的配合。

假如在 IIS 服务器中有一网站 www.lnpc.cn，对应 IP 地址为 192.168.13.200，端口号为 80。video.lnpc.cn 网站还未建立。下面简单介绍在 IIS 服务器上这两个网站的建立过程。

步骤 1：在"DNS 管理器"中找到"正向查找区域"下的 lnpc.cn 区域，在右边的 support 记录上右击，选择弹出菜单"属性"，在打开的"support 属性"窗口中，把 IP 地址改为 192.168.13.200。这时两个记录都指向 192.168.13.200，如图 11-26 所示。

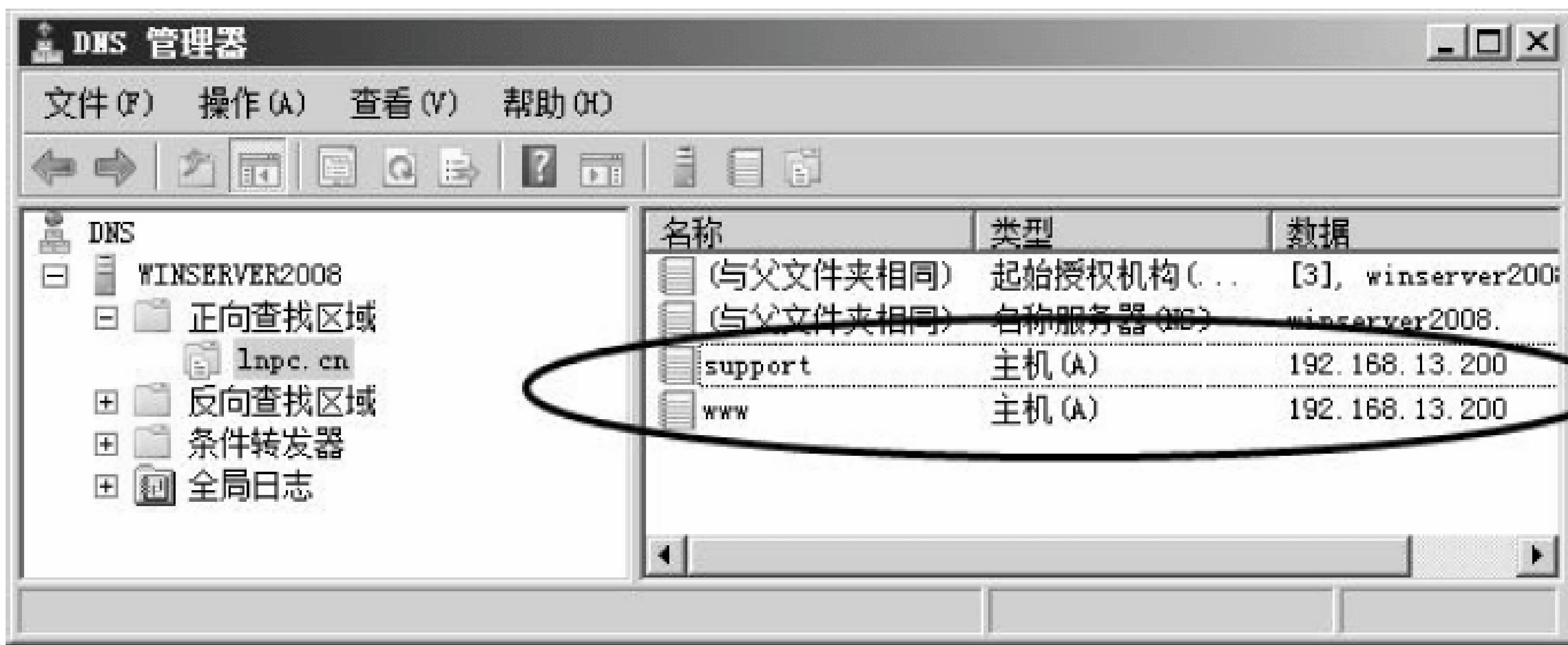



图 11-26　DNS 中建立的两个记录

步骤 2：已有网站的设置

"Internet 信息服务(IIS)管理器"中选中 Default Web Site 网站，右击，选择弹出菜单"编辑绑定"，在弹出的"网站绑定"窗口中，选择网站，单击"编辑"按钮，弹出"编辑网站绑定"窗口，把 IP 绑定 192.168.13.200，端口设置为 80，主机名设为 www.lnpc.cn，如图 11-27 所示。




图 11-27　编辑已有网站的绑定

步骤 3：新建网站

“Internet 信息服务(IIS)管理器”中选中“网站”，右击，选择弹出菜单“添加网站”，在打开的窗口中，输入网站名称 video，物理路径 C:\video，IP 地址为 192.168.13.200，端口为 80，主机名为 video.lnpc.cn，主机名很重要，如图 11-28 所示。




图 11-28　新建网站

步骤 4：设置默认文档。选择新建的网站，双击中间窗格中的默认文档，设置 video 网站的默认文档。

步骤 5：打开浏览器验证两个网站。由于连接时，发送到 IIS 服务器的数据包除了 IP 地址以外，还包括网址（www. lnpc. cnt 和 video. lnpc. cn），IIS 服务器在对比网址和域名以后，就知道要连接的网站了，如图 11-29 所示。




图 11-29 不同域名的网站测试

# 11.4 IIS 服务器的安全

Windows Server 2008 中的 IIS 采用模块化设计，默认采用最小化安装，用户根据需要自己安装和卸载各模块。这样可以减少 IIS 遭受攻击的可能性。

## 11.4.1 用户身份的验证

IIS 默认允许所有用户访问网站，为了提高系统的安全性，可以对用户的身份做一些限制，比如只允许特定用户登录网站，验证不合格的用户不允许访问网站。

**1. IIS 服务器用户验证方式**

1）匿名身份验证

匿名身份验证允许任何用户访问任何公共内容，而不用向客户端浏览器提供用户名和密码质询。默认情况下，匿名身份验证在 IIS 7.0 中处于启用状态。

2）基本身份验证

基本身份验证要求用户在访问内容时提供有效的用户名和密码。所有主流的浏览器都支持该身份验证方式，它可以跨防火墙和代理服务器工作。基本身份验证的缺点是它使用弱加密方式在网络中传输密码。只有当知道客户端与服务器之间的连接是安全连接时，才

能使用基本身份验证。

3）摘要式身份验证

摘要式身份验证也要求用户输入用户名和密码，不过在网络上发送的是经过 MD5 处理过的摘要值，这个值即使被别人获得，他也无从得到原始的用户名和密码，因此，比使用基本身份验证安全得多。另外，当今所有浏览器都支持摘要式身份验证，摘要式身份验证可以通过代理服务器和防火墙来工作。

4）Windows 身份验证

Windows 身份验证的用户名和密码也是经过哈希处理的，因此较为安全。Windows 身份验证适用于内部网或企业的 Intranet。

**2. 身份验证组件的安装**

步骤 1：依次选择“开始”→“管理工具”→“服务器管理器”。

步骤 2：打开“服务器管理器”窗口，在左侧窗格中选择“角色”下的“Web 服务器”，在右侧单击“添加角色服务”。

步骤 3：在“添加角色服务”窗口中，选中安全性下的所有组件，如图 11-30 所示。

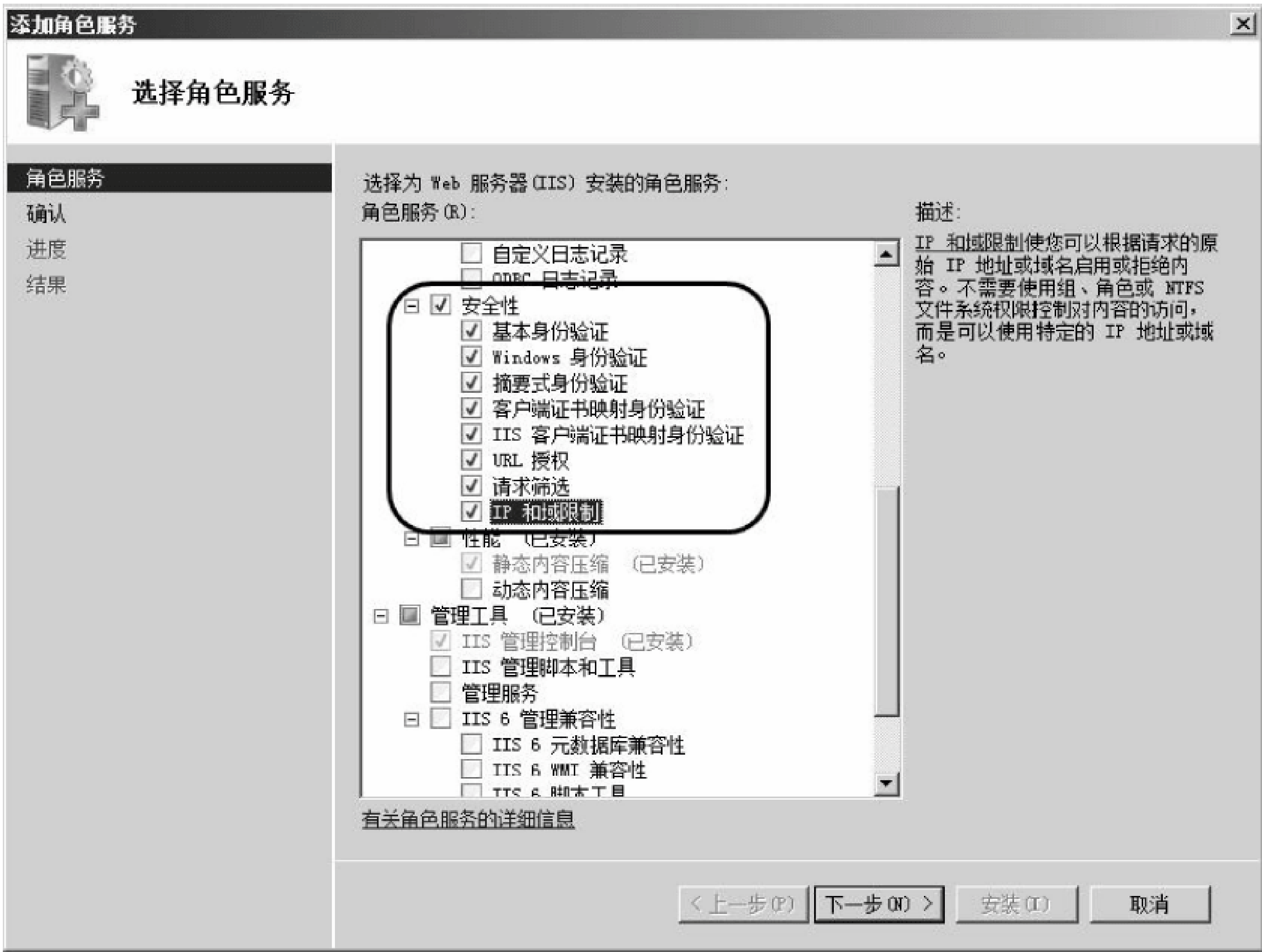



图 11-30　IIS 服务器安全组件的安装

步骤 4：按照向导指示，完成组件的安装。

**3. 验证用户身份**

如果要对网站或网站下的文件、文件夹实施保护，可以进行用户名和口令的验证，下面

以 Default Web Site 网站为例，讲述网站身份验证的过程。

在"Internet 信息服务(IIS)管理器"中选择左侧的 Default Web Site，双击中间功能窗格中的"身份验证"。打开如图 11-31 所示界面。




图 11-31 IIS 身份验证方式

选"匿名身份验证"，单击右侧的禁用，再选择"Windows 身份验证"，单击右侧的"启用"，这时就禁用了匿名身份验证，而启用了 Windows 身份验证。

在客户端打开浏览器，输入 www.lnpc.cn 网址，浏览器出现一个身份验证窗口，输入正确的用户名和密码后，方能访问网站，如图 11-32 所示。

若输入的用户名和密码不正确则会显示未经授权错误信息，如图 11-33 所示。




图 11-32 网站的身份验证界面

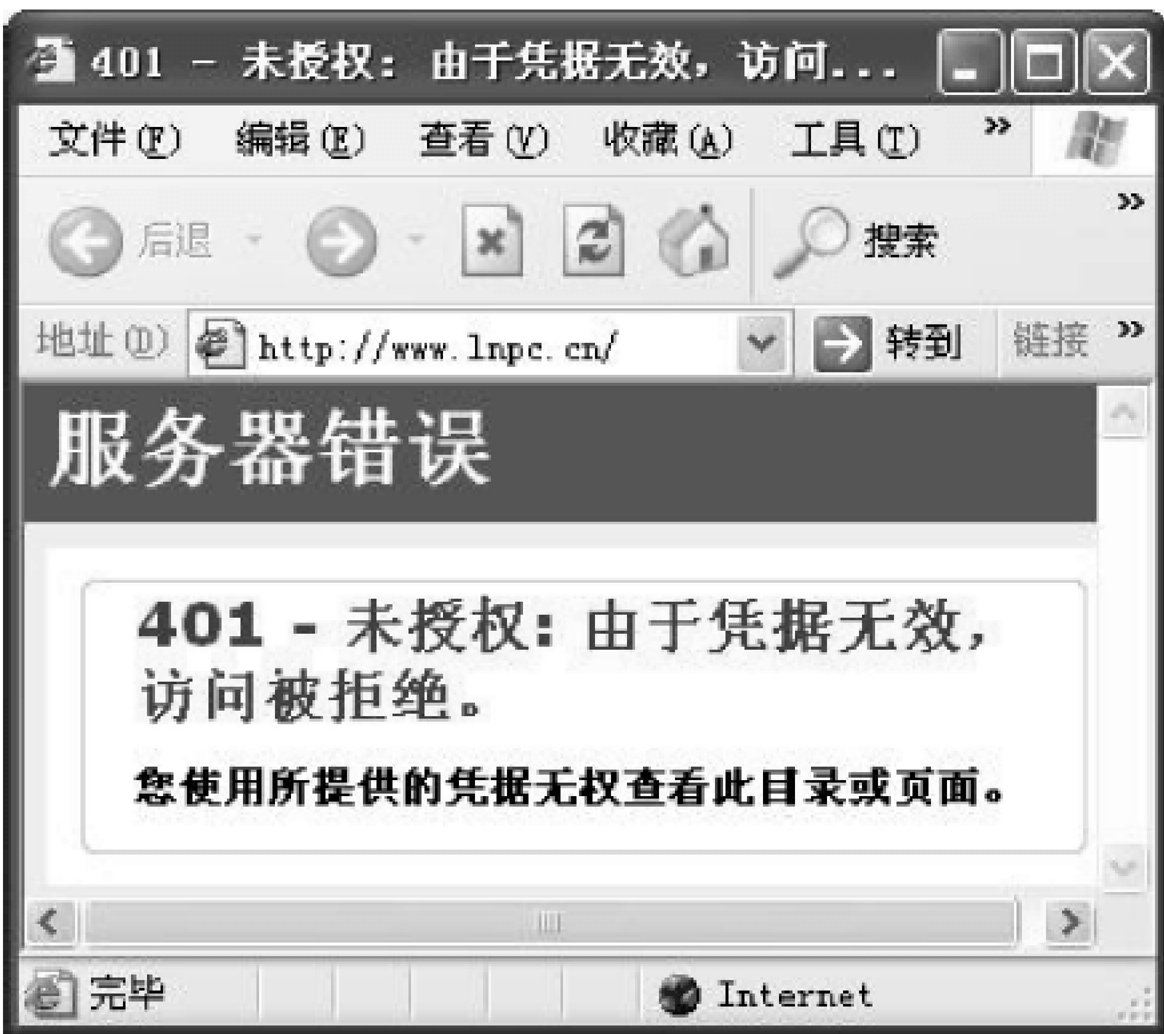



图 11-33 验证错误界面

### 11.4.2　通过 IP 地址限制连接

IIS 可以为特定 IP 地址、IP 地址范围或域名定义和管理允许或拒绝访问内容的规则。例如校园网中的 IIS 服务器通过设置允许校园网中的用户连接到 Web 服务器，而不允许其他用户连接上来。实现此功能必须安装 IIS 组件：IP 和域限制。其安装过程与 11.4.1 节中其他安全组件的安装过程相似，只是在安装时选择“IP 和域限制”，这里就不再说明具体安装过程。下面以 Default Web Site 网站为例说明 IIS 连接限制的设置过程。

打开“Internet 信息服务(IIS)管理器”中选择左侧的 Default Web Site 网站，如图 11-34 所示。




图 11-34　IP 地址和域限制

在中部“功能窗格”中双击“IPv4 地址和域限制”，切换到如图 11-35 所示的 IP 地址和域限制条目界面。

在图 11-35 界面右侧，单击“添加允许条目”可以添加允许访问网站的条目。如本例中允许 192.168.13 子网的客户访问网站，如图 11-36 所示。

在图 11-35 界面右侧，单击“添加拒绝条目”可以添加拒绝访问网站的条目。如本例中拒绝 192.168.13.201 客户的访问，如图 11-37 所示。

如果从被拒绝的 IP 地址访问网站，则会显示禁止访问的信息，如图 11-38 所示。




图 11-35 规则添加界面

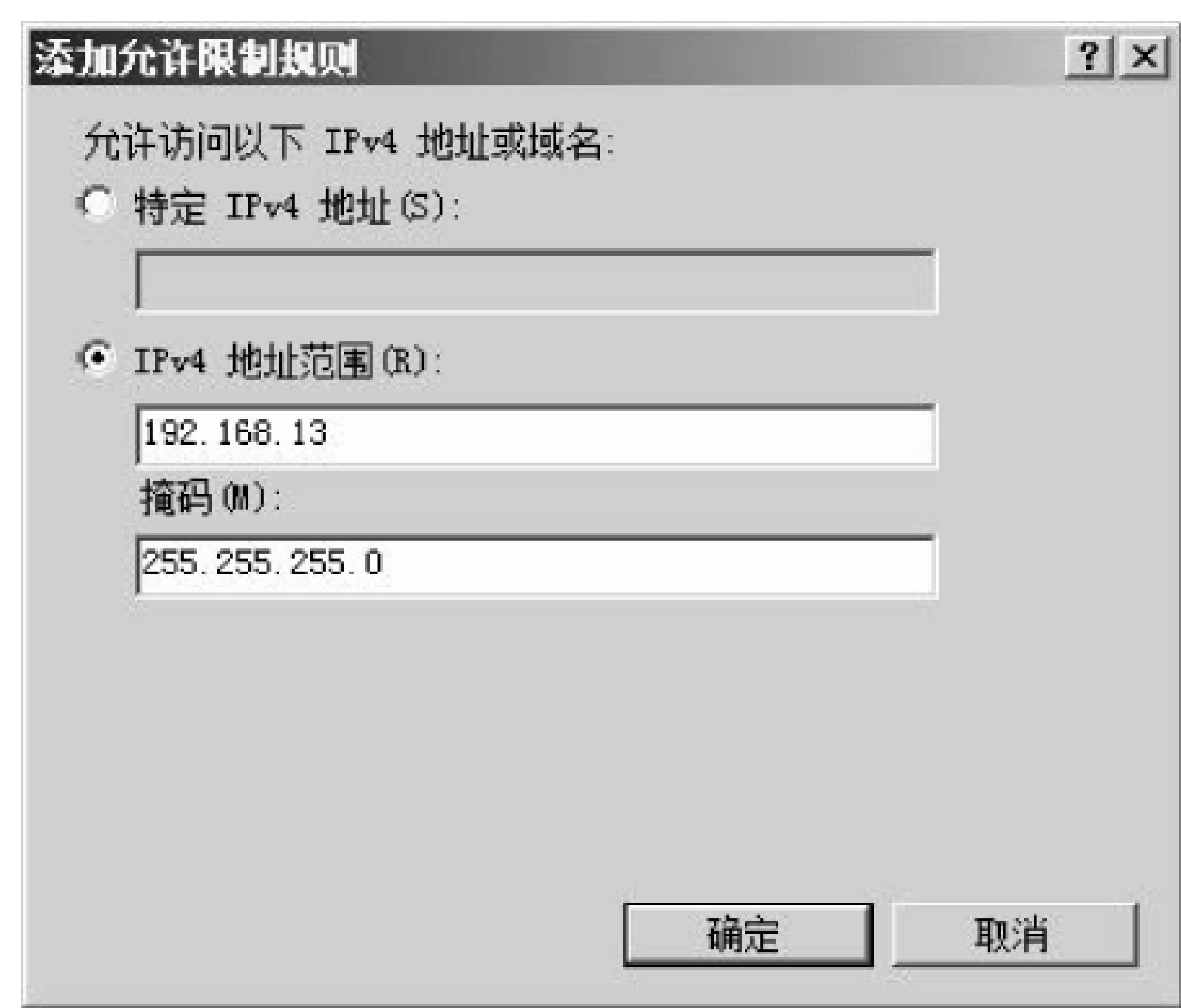



图 11-36 添加允许访问网站的网段

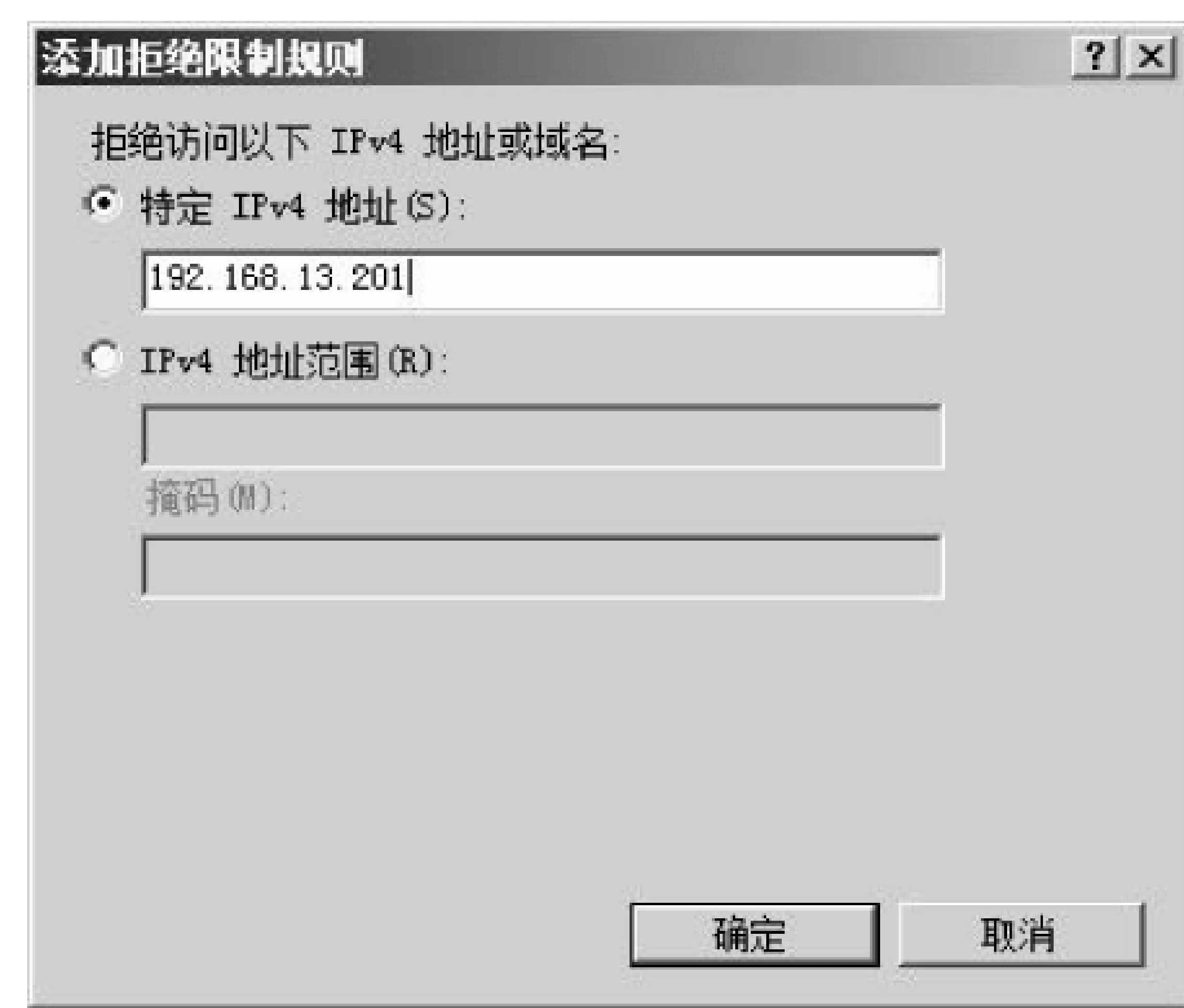



图 11-37 添加拒绝访问网站的 IP 地址




图 11-38 访问网站被拒绝的界面

# 实验 16　Web 服务器的配置

**1. 实验目标**

(1) 掌握 Web 服务的工作原理。

(2) 掌握 Windows Server 2008 下 Web 服务器的配置方法。

**2. 实验准备**

两台安装了 Windows Server 2008 的服务器或者一台安装了虚拟机的性能较好的计算机。

**3. 实验内容**

(1) 练习在一台服务器的不同 IP 地址上架设不同网站。在装有 Windows Server 2008 的服务器上绑定 IP 地址 192.168.1.1,192.168.1.2,192.168.1.3,分别架设"新闻网站"、"视频点播网站"、"运动网站"。

(2) 练习在一台服务器的不同端口上架设不同网站。在装有 Windows Server 2008 的 Web 服务器上架设两个网站:一个占用服务器的 80 端口,一个占用 8080 端口。

(3) 练习在一台服务器上根据主机头架设不同网站。

① 在一台装有 Windows Server 2008 的计算机上架设 Web 服务器,其 IP 地址是 192.168.1.1,并在其上架设三个网站:news.xyz.com,vod.xyz.com,sports.xyz.com。

② 在另一台服务器上架设 DNS 服务器,其 IP 为 192.168.1.100,在 DNS 服务器上建立 xyz.com 域,建立 news.xyz.com,vod.xyz.com,sports.xyz.com 域名对应 IP 地址 192.168.1.1。

③ 用域名 news.xyz.com,vod.xyz.com,sports.xyz.com 访问三个网站。

# 思考与练习

**一、填空题**

1. Web 服务的特点为________,________,________和________。

2. 目前市场占有率排名前三名的 Web 服务器是________,________和________。

3. IIS 服务器用户身份验证方式包括________,________,________和________。

**二、选择题**

1. 下面关于 HTTP 协议错误的描述是(　　)。

　A. Web 服务器和浏览器通信是基于 HTTP 协议

　B. HTTP 协议默认端口是 8080

　C. HTTP 协议采用的是请求/响应模型

　D. HTTP 协议默认端口是 80

2．在 IIS 服务器中使用虚拟目录的优点不包括(　　)。

A．提高 Web 服务器的安全性

B．提高网站建设的灵活性

C．均衡服务器的负载

D．提高服务器的服务质量

3．在一台 IIS 服务器中实现多网站发布不包括以下(　　)技术。

A．使用不同的 IP 发布不同的网站

B．使用不同的端口发布不同的网站

C．使用不同的主机标识名发布不同的网站

D．根据不同的客户端的 IP 地址发布不同的网站

**三、思考题**

1．什么是 Web？它的主要特点是什么？

2．Internet 服务器管理器的功能有哪些？

3．建立和管理 Web 网站有哪些主要步骤？

4．什么叫虚拟目录？它有什么作用？

5．IIS 用什么途径提高网站的安全性？

第 12 章

# FTP 服务器的配置与管理

## 12.1 FTP 概 述

### 12.1.1 FTP 简 介

FTP 是 File Transfer Protocol 的缩写，即文件传输协议。FTP 用于网络中文件的传输，既可以把文件上传到服务器，也可以把文件下载到本地客户机。它独立于操作系统，不管是在 Windows 中还是在 UNIX、Linux 或 Mac 操作系统中都能使用。FTP 位于网络的应用层，采用面向连接的 TCP 协议，而非 UDP 协议，所以能保证传输数据的正确性。

但 FTP 服务也存在着明显的缺点。

(1) 密码和文件内容都使用明文传输，可能产生不希望发生的窃听。

(2) 因为必须开放一个随机的端口以建立连接，当防火墙存在时，客户端很难过滤处于主动模式下的 FTP 流量。这个问题通过使用被动模式的 FTP 得到了解决。

(3) 服务器可能会被告知连接一个第三方计算机的保留端口。

FTP 中采用两个独立的 TCP 连接通道：一个是用于传输命令的控制通道，通常使用 21 号端口；另一个是用于传输数据的数据通道，通常使用 20 号端口。控制通道使用较小的带宽，延迟较小，而数据通道使用的带宽较大，相对延迟较大。

针对 FTP 的数据通道而言有两种传输模式：主动传输模式和被动传输模式。

**1. 主动传输模式**

FTP 服务器一直在监听 21 号端口，客户端向服务器端 21 号端口发出连接请求，双方通过身份验证后，建立起控制连接，但双方的数据连接并未建立。当 FTP 客户端要列目录、上传或下载数据时，客户端通过控制连接向服务器发出 PORT 加端口的命令，请求服务器与客户端的那个指定端口建立数据连接，服务器端主动使用 20 号端口与客户端的指定端口建立连接，进行数据传输。比如，客户端向服务器端发出 PORT 加 1344 端口号命令，服务器主动从 20 号端口与客户端的 1344 号端口建立了数据连接。

**2. 被动传输模式**

当客户端与服务器端的控制连接建立起来以后，客户端要列目录、上传或下载数据时，客户端向服务器端发出 PASV 命令，服务器接到这个命令后，用 PORT 加端口号响应客户端，然后，客户端通过服务器指定的端口与服务器建立连接，服务器在整个过程中处于被动

等待状态。因此，把这种状态称为被动传输模式，也叫 PASV 模式。比如客户端从 1240 向服务器端 21 号发出 PASV 命令，服务器端向客户端发出 PORT 加 2040 端口号响应，客户端主动从 1241 端口与服务器的 2040 端口建立数据连接。

## 12.1.2 FTP 软件的安装

Windows Server 2008 发布的时候，没有集成 FTP for IIS 7.0，而使用了 FTP for IIS 6.0。后来又发布了 FTP 7.5 for IIS 7.0。所以，在 Windows Server 2008 中可以使用两个版本的 FTP 软件。这里我们以后发布的 FTP 7.5 for IIS 7.0 为例讲解 FTP 软件的配置与应用。

Microsoft FTP Service 7.5 for IIS 7.0 的下载地址为：

http://www.microsoft.com/download/en/default.aspx。

在搜索栏中，输入 FTP IIS7，即可找到。软件分为两个版本，一个是 32 位版，一个是 64 位版。32 位版的下载地址为：

http://www.microsoft.com/download/en/details.aspx? id=14045。

下载的文件名为 ftp7_x86_75.msi。

64 位版的下载地址为：

http://www.microsoft.com/download/en/details.aspx? id=22045。

下载的文件名为 ftp7_x64_75.msi。

根据自己所使用 Windows Server 2008 的版本下载相应 FTP 软件，双击后，一路“接受”或“下一步”即可完成安装。安装后的 Internet 信息(IIS)管理器界面如图 12-1 所示。




图 12-1 安装 FTP 软件后的 IIS 管理器界面

| | |
|---|---|
| FTP Authentication | FTP 身份验证 |
| FTP Authorization Rules | FTP 授权规则 |
| FTP Directory Browsing | FTP 目录浏览 |
| FTP Firewall Support | FTP 防火墙支持 |
| FTP IPv4 Address and Donain Restrictions | FTP IPv4 地址和域名限制 |
| FTP Logging | FTP 日志 |
| FTP Messages | FTP 消息 |
| FTP Request Filting | FTP 请求过滤 |
| FTP SSL Settings | FTP SSL 设置 |
| FTP User Isolation | FTP 用户隔离 |

## 12.2　FTP 服务器的配置

### 12.2.1　建立匿名登录的 FTP 站点

步骤 1：依次选择"开始"→"管理工具"→"Internet 信息服务(IIS)管理器"。

步骤 2：在"Internet 信息服务(IIS)管理器"左侧"连接"窗格选择"网站"，在右侧"操作"窗格，选择 Add FTP Site…，如图 12-2 所示。




图 12-2　添加 FTP 站点

步骤 3：在打开的 Add FTP Site 窗口中，输入 FTP 站点的名称 myftp，输入或单击".."按钮选择 FTP 站点的物理位置。单击"下一步"按钮，如图 12-3 所示。

步骤 4：在 Binding and SSL Settings 窗口中，单击 IP Address 下拉列表框，选择服务器绑定的 IP 地址；在 Port 文本框中为 FTP 服务器使用的端口，这里使用默认值 21；因为该网点并未拥有 SSL 证书，因此，选择 No SSL。单击"下一步"按钮，如图 12-4 所示。

步骤 5：因为此站点要让匿名用户访问，在 Authentication 中选择 Anonymous(匿名)、Basic；在 Authorization 中选择 Anonymous users；在 Permissions 中选择 read。单击"完成"按钮，如图 12-5 所示。

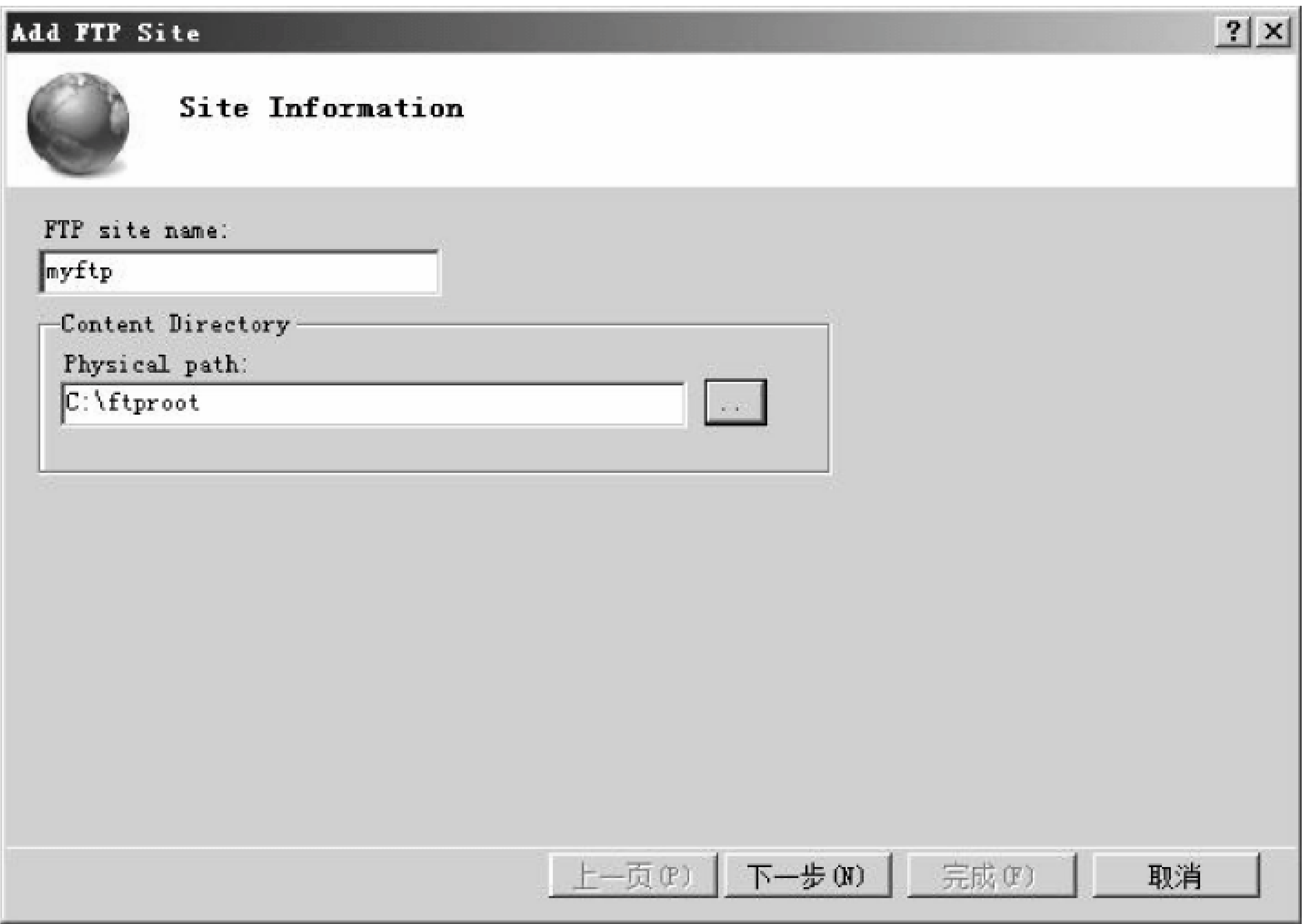



图 12-3　输入 FTP 信息

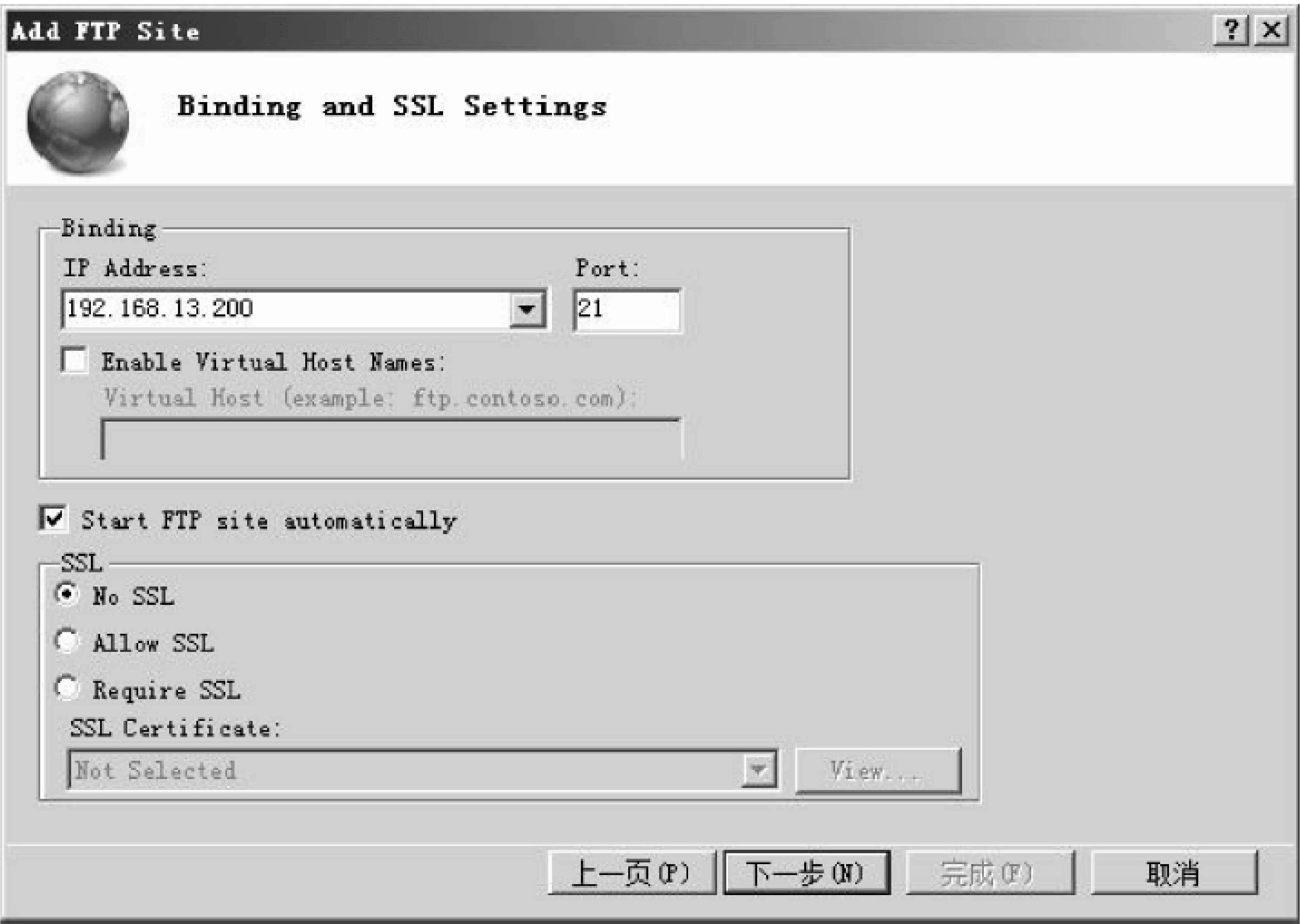



图 12-4　绑定 IP 和设置 SSL

## 12.2.2　FTP 站点测试

对于 FTP 站点的测试有多种方法：命令行下的 FTP 命令；浏览器；FTP 客户端工具。下面分别予以介绍。




图 12-5　设置验证和授权

### 1. 命令行命令测试

在 Windows 命令行下有 ftp. exe 程序,该程序能够实现 FTP 的基本功能。FTP 命令使用主动传输模式,使用 21 号端口进行命令传输,用 20 号端口进行数据传输。依次选择“开始”→“运行”,在对话框中输入 cmd,单击“确定”按钮,打开命令行窗口。输入 FTP 即可执行,在 ftp 提示符下输入? 即可显示 FTP 命令。输入 ftp 192. 168. 13. 200,然后输入用户名 anonymous,密码为空,即可登录 FTP 服务器,输入 dir 进行资源列表,quit 或 bye 退出 FTP,如图 12-6 所示。

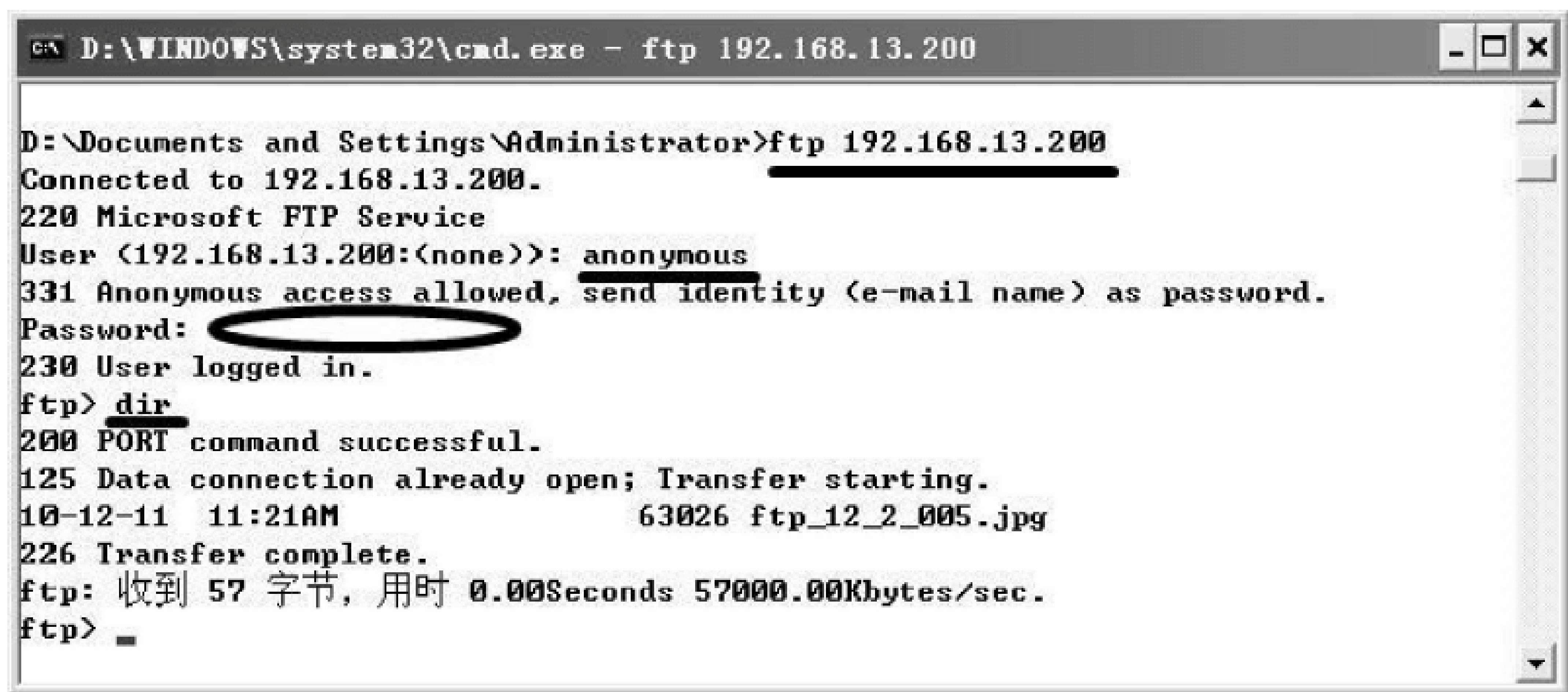



图 12-6　命令行下的 ftp 命令

### 2. 浏览器测试

打开浏览器,在地址栏输入 ftp://192. 168. 13. 200,浏览器中会显示 FTP 服务器中的

资源，在资源上右击，选择弹出菜单中的“复制到文件夹”，把文件复制到某一文件夹即完成FTP文件的下载，如图12-7所示。

**3. FTP客户端软件测试**

现在FTP客户端软件有很多，既有商业化软件，也有开源的免费软件。下面以开源免费的FileZilla为例加以说明。FileZilla下载地址为http://sourceforge.net/projects/filezilla/。打开软件后，主机栏输入192.168.13.200，用户名输入anonymous，密码为空，端口为21。窗口中部左侧为客户端本地文件，中部右侧为FTP服务器上的文件，把文件从右侧拖到左侧即是下载文件，把文件从左侧拖到右侧即为上传，如图12-8所示。




图12-7 浏览器测试FTP服务




图12-8 FTP客户端工具测试

## 12.2.3 FTP服务器的基本设置

**1. FTP服务的启动与停止**

(1) 在“Internet信息服务(IIS)管理器”中，选中FTP服务器站点myftp，窗口右侧“操作”窗格中有Restart、Start、Stop选项，单击即可执行相应动作，如图12-9所示。




图 12-9　从 IIS 管理器启动/停止 FTP 服务

(2) 启动/停止 FTP 服务。

依次选择"开始"→"管理工具"→"服务",选择 Microsoft FTP Service,单击工具栏上的按钮;或单击窗口中部的文字;或右击服务名,选择弹出菜单中的相应选项,如图 12-10 所示。

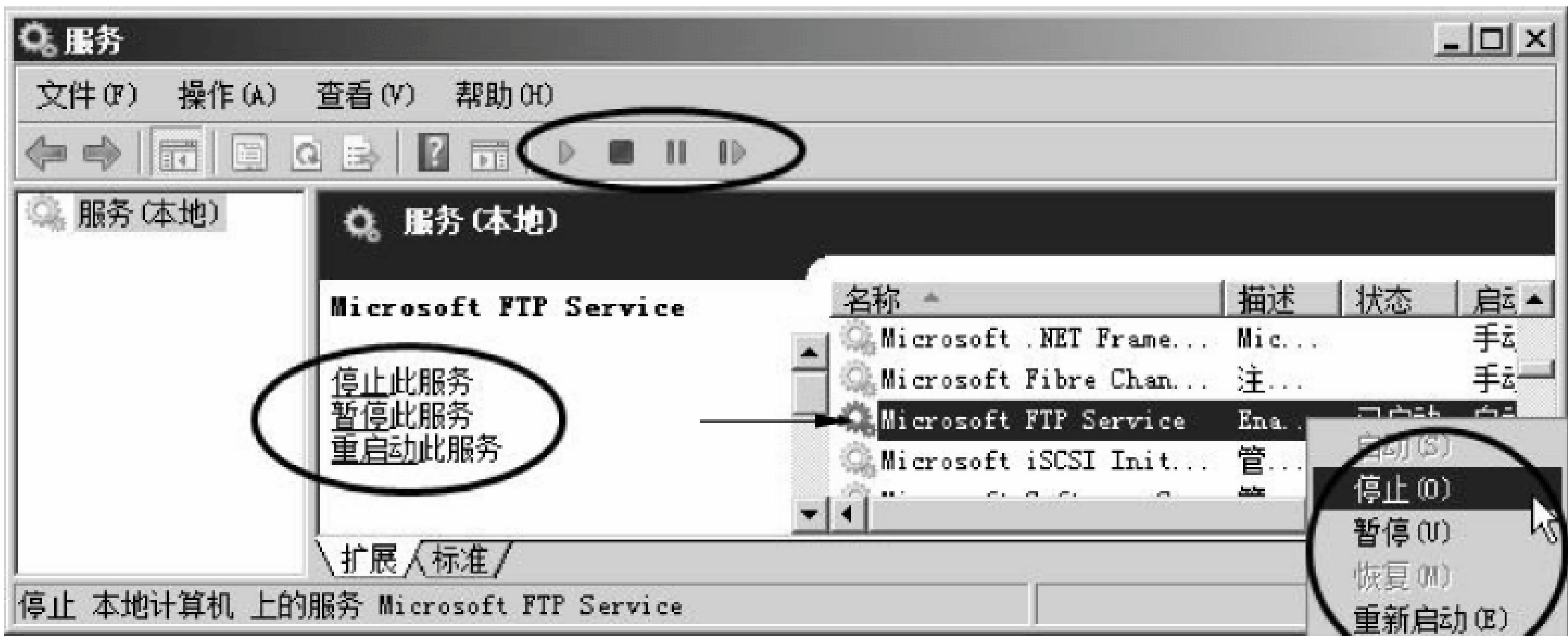



图 12-10　启动/停止 FTP 服务

## 2. 查看 FTP 服务器当前登录用户

在"Internet 信息服务(IIS)管理器"窗口中选择 FTP 站点 myftp,单击 FTP Current Sessions,中部窗格即显示当前连接到 FTP 服务器的用户信息,如图 12-11 所示。

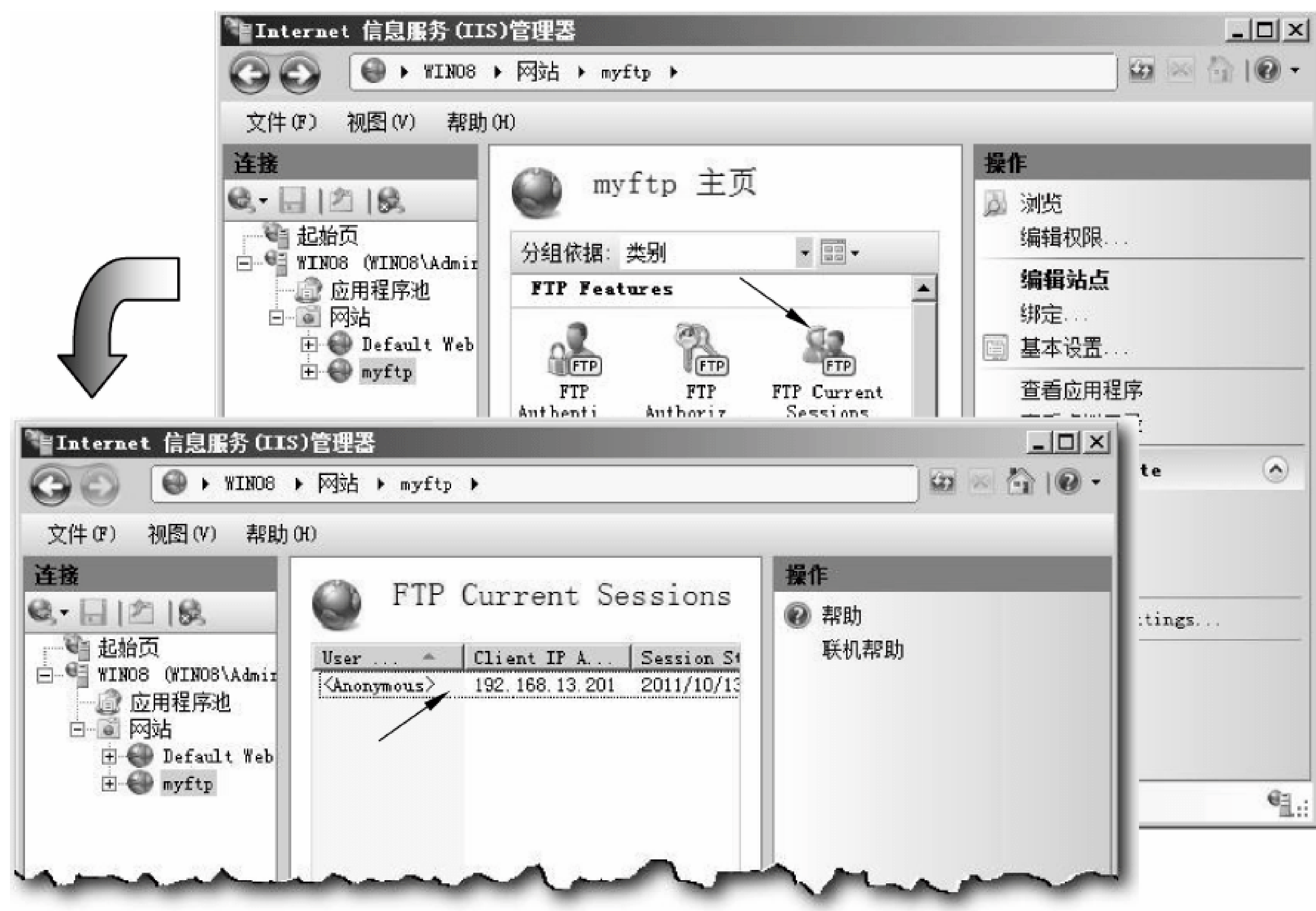


图 12-11　查看当前连接到 FTP 服务器的用户

**3. FTP 站点文件存储位置**

FTP 服务器中的文件是被存储在 FTP 服务器的主目录中的，在创建 FTP 站点时已经设置了主目录的位置，创建站点以后还可以修改主目录位置。在“Internet 信息服务(IIS)管理器”左侧窗口中选择 FTP 站点，在右侧的“操作”窗格中选择“基本设置”。打开“编辑网站”窗口，在物理路径中输入或单击“..”按钮选择 FTP 站点物理存储路径。这样可以把 FTP 文件存储的位置改变到本服务器的其他位置或网络上其他计算机的共享文件夹，如图 12-12 所示。

**4. FTP 站点绑定设置**

在“Internet 信息服务(IIS)管理器”窗口中选择 FTP 站点 myftp，单击右侧“操作”窗格“绑定”，打开“网站绑定”窗口，选择列表框中的 FTP 服务，单击“编辑”，打开“编辑网站绑定”窗口，在这里可以绑定三种信息：IP 地址、端口、主机名。和第 11 章中介绍的网站绑定类似，用户可以通过三种途径访问到 FTP 服务器，如图 12-13 所示。

**5. FTP 信息的设置**

FTP 服务器可以设置各种信息，比如横幅、欢迎、退出等信息，当用户执行某个动作时，在客户端显示相应的信息。

在“Internet 信息服务(IIS)管理器”窗口中选择 FTP 站点 myftp，双击中部“功能”窗格中的 FTP Messages，即可打开设置界面，如图 12-14 所示。



图 12-12　设置 FTP 文件存储位置



图 12-13　FTP 站点绑定设置

FTP 信息包括内容如下。

Banner：用户连接到服务器时，首先看到的信息。此信息最好是英文字符。




图 12-14 设置 FTP Messages

Welcome：用户登录服务器时显示的欢迎信息。

Exit：用户退出 FTP 服务器时显示的退出信息。

具体如图 12-15 所示。




图 12-15 FTP 信息设置

图 12-15 中可以看出还有三个选项如下。

Suppress default banner：隐藏默认横幅，图 12-16 中的 Microsoft FTP Service 就是默认横幅，如果选中在客户端即不显示 Microsoft FTP Service




图 12-16　FTP 登录后的信息

Support user variables in messages：在信息中支持用户变量。如图 12-17 和图 12-18 所示，用户变量包括：%BytesReceived%，%BytesSent%，%SessionID%，%SiteName%，%UserName%。




图 12-17　带变量的 FTP 信息设置




图 12-18　带变量的 FTP 信息显示结果

Show detailed messages for local requests：本地登录时，若连接有误，显示详细信息。从其他计算机连接时不会显示错误信息。

# 12.3　FTP 站点的架设

## 12.3.1　创建集成到 IIS 网站的 FTP 站点

FTP 7.5 for IIS 7.0 有效地融入到了 IIS 7.0 中，将 Web 服务和 FTP 服务集成为一体，这样 Web 网站管理员就可以利用 FTP 进行网站管理了。下面简单介绍一下 FTP 服务集成到 IIS 的过程。

步骤 1：打开"Internet 信息服务(IIS)管理器"，单击"网站"下的 Default Web Site，单击 Add FTP Publishing，如图 12-19 所示。

步骤 2：在打开的 Add FTP Publishing 窗口 IP Address 下拉列表框中选择 FTP 服务器的 IP，Port 输入 FTP 服务器的端口，SSL 选择框中选择是否使用 SSL。由于以前建立的 myftp 站点使用 192.168.13.200 地址和 21 号端口。IP 地址、端口号和虚拟主机名等三个值要与以前的设置不同，否则 FTP 站点无法启动。为避免冲突这里使用 2121 号端口。单击"下一步"按钮。

步骤 3：在打开的 Authentication and Authorization Information 中，选择 Basic 验证方式，选择 Specified users 授权方式，在下面填入 tom 用户名，这里的用户名是在"控制面板"→"用户账户"→"管理其他账户"→"创建一个新账户"创建的本地账户，如图 12-20 所示。

步骤 4：安装完成后，用户就可以使用客户端工具进行 Web 网站文件的下载和上传管理了。

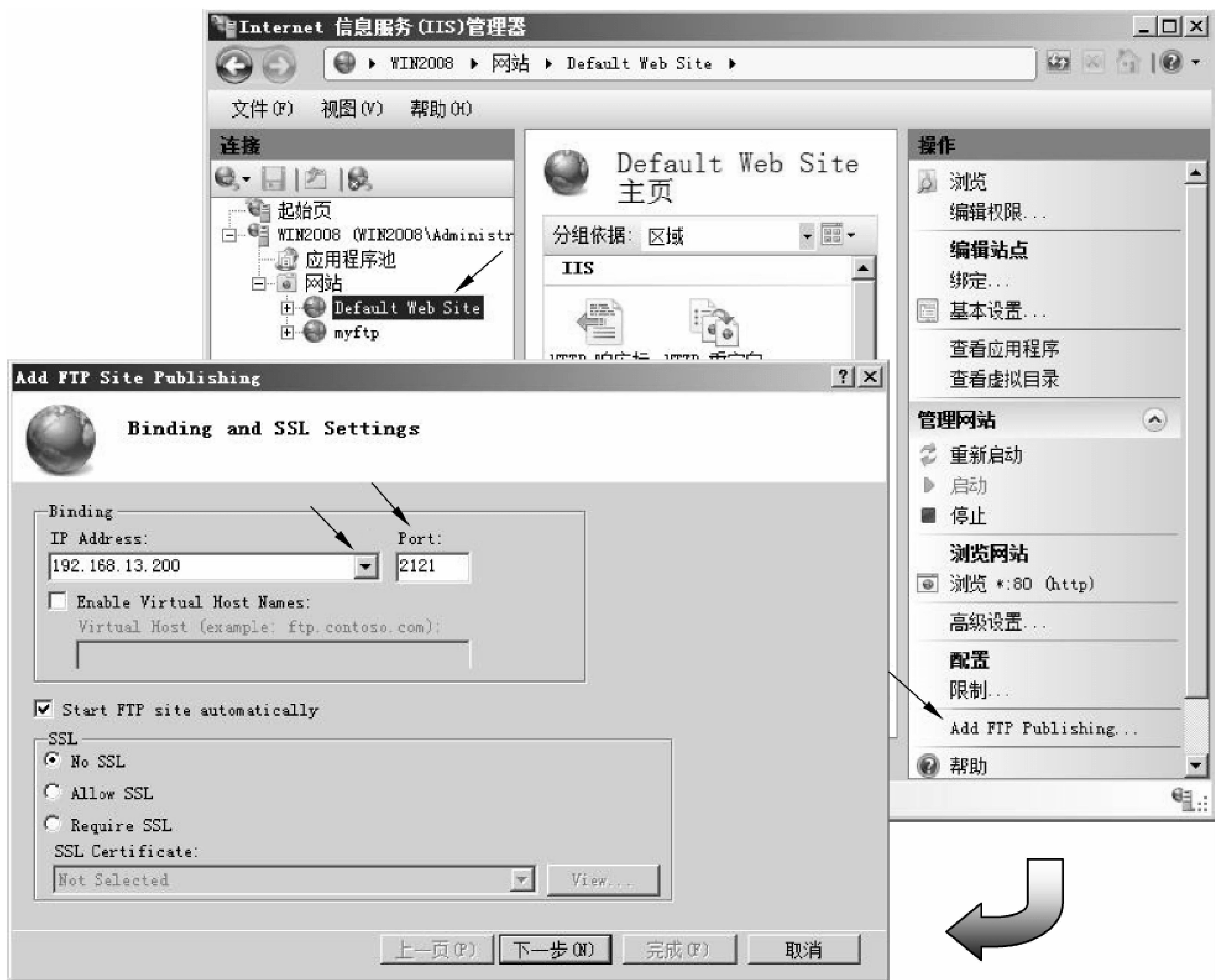



图 12-19　为 IIS 添加 FTP 服务

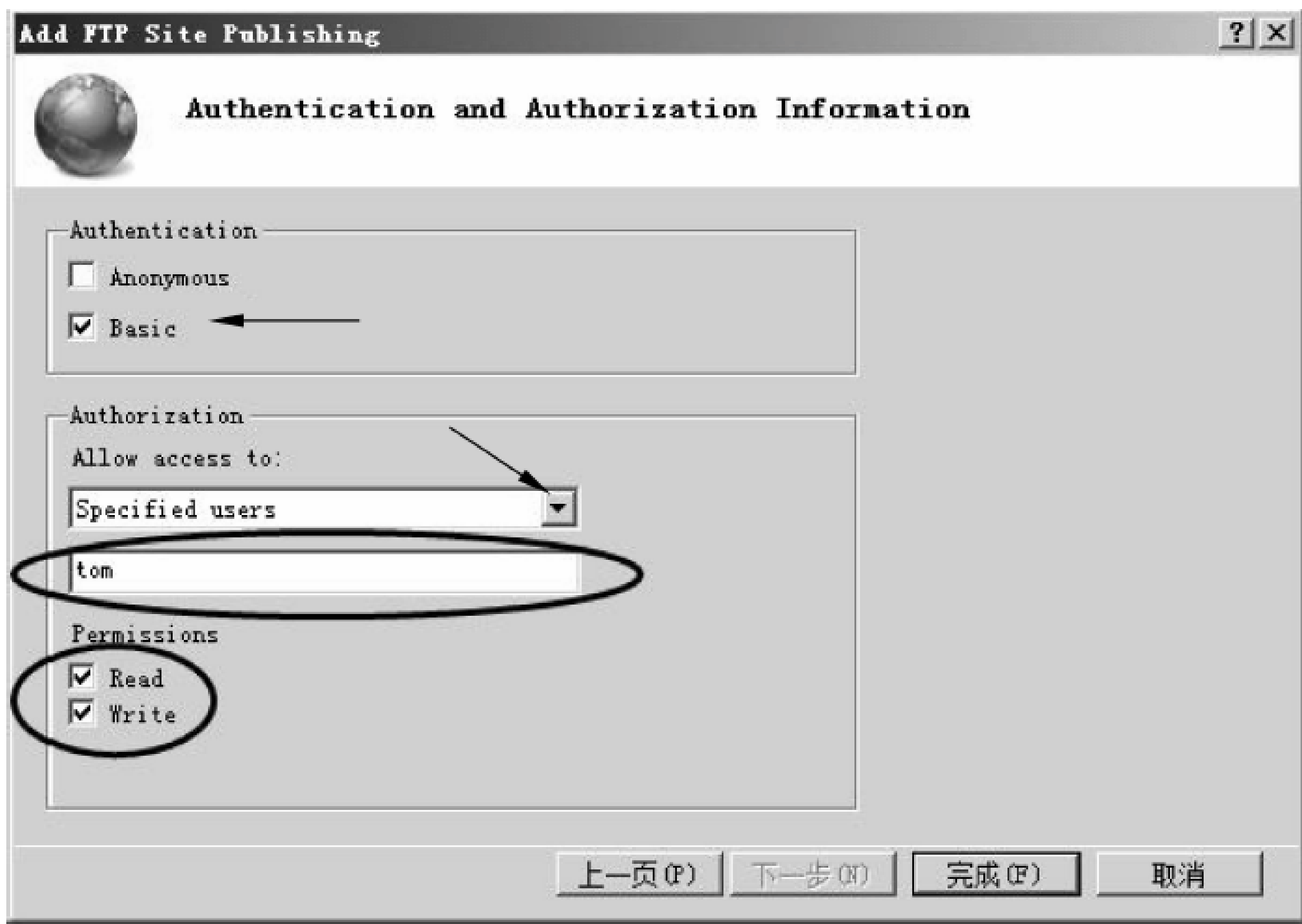



图 12-20　FTP 站点验证与授权设置

## 12.3.2 虚拟目录的设置

在一个 FTP 站点下可能有多个子目录，分门别类地存放着不同的 FTP 资源，这些文件资源不一定都要存储在 FTP 的主目录中，它们可以存储在不同的文件夹下，例如存储在本地计算机的其他分区中或者网络中其他计算机的共享文件夹中。这样的 FTP 子目录称为 FTP 虚拟目录或别名。只要别名不变，无论物理目录如何变化，用户可以通过别名来访问子目录下的文件。下面以在 myftp 站点下建虚拟目录 image 为例，介绍虚拟目录的建立。

步骤 1：打开“Internet 信息服务(IIS)管理器”，右击“网站”下的 myftp，选择弹出菜单中的“添加虚拟目录”，如图 12-21 所示。或者单击 myftp 站点，单击中部窗格下方的“内容视图”，切换到内容视图，这时右部窗格会有“添加虚拟目录”，单击即可打开图 12-22 所示界面。




图 12-21 添加虚拟目录




图 12-22 设置虚拟目录

步骤 2：打开“添加虚拟目录”对话框，在“别名”框中，输入 image 作为别名，输入物理路径“C:\image”或单击“..”选择“C:\image”。单击“确定”按钮。

步骤 3：在“Internet 信息服务(IIS)管理器”窗口中，单击“网站”下的 myftp，双击中部功能窗格中的 Directory Browsing。中部窗格变为 FTP Directory Browsing。

步骤 4：选择 Directory Listing Options 中的 Virtual Directories，如图 12-24 所示，只有选择了此选项，客户端才能显示虚拟目录。单击右侧“操作”窗格中的“应用”，保存设置。




图 12-23　选择 FTP Directory Browsing




图 12-24　选中 Virtual Directories

### 12.3.3 创建多个 FTP 站点

在同一个网络 FTP 服务器中可以创建多个虚拟站点，通过 IP 地址、端口、主机域名三种途径可以区分开不同的 FTP 站点，也就是说通过这三种方式创建不同的 FTP 站点。

**1. 通过不同的 IP 地址创建不同的站点**

通过不同的 IP 地址创建不同的 FTP 站点，服务器必须拥有多个 IP 地址，服务器绑定多个 IP 地址的方法参见 11.3.1 小节。创建 FTP 站点并绑定指定 IP 地址的方法请参见 12.2.1 小节。新创建的每个 FTP 站点绑定一个不同的 IP 地址，端口采用相同的 21 号端口。客户端在浏览器中访问 FTP 服务器时采用"ftp://IP 地址"的方式，不同的 IP 访问不同的站点。

**2. 通过不同的端口访问创建不同的站点**

创建站点的方法请参见 12.2.1 小节，绑定端口请参见 12.2.3 小节，在设置站点端口时，请注意不同站点设置为不同的端口。客户端使用浏览器访问 FTP 站点的方法是："ftp://192.168.13.200:2121"，其中 2121 是 FTP 站点的端口，不同站点的端口是不同的。

**3. 通过不同域名创建不同 FTP 站点**

FTP 7.5 for IIS 7.0 可以通过不同域名创建不同 FTP 站点，但是 Windows Server 2008 自带的 FTP for IIS 6.0 不具有这个功能，下面简要介绍 FTP 站点创建过程。

步骤 1：在 DNS 服务器中创建两个域名为 tools.lnpc.cn，film.lnpc.cn。它们映射的 IP 地址都是 192.168.13.200。

步骤 2：在"Internet 信息服务(IIS)管理器"左侧"连接"窗格选择"网站"，在右侧"操作"窗格，选择 Add FTP Site。

步骤 3：在打开的 Site Information 对话框中，输入站点名称为 tools，物理路径为 C:\tools，单击"下一步"按钮，如图 12-25 所示。

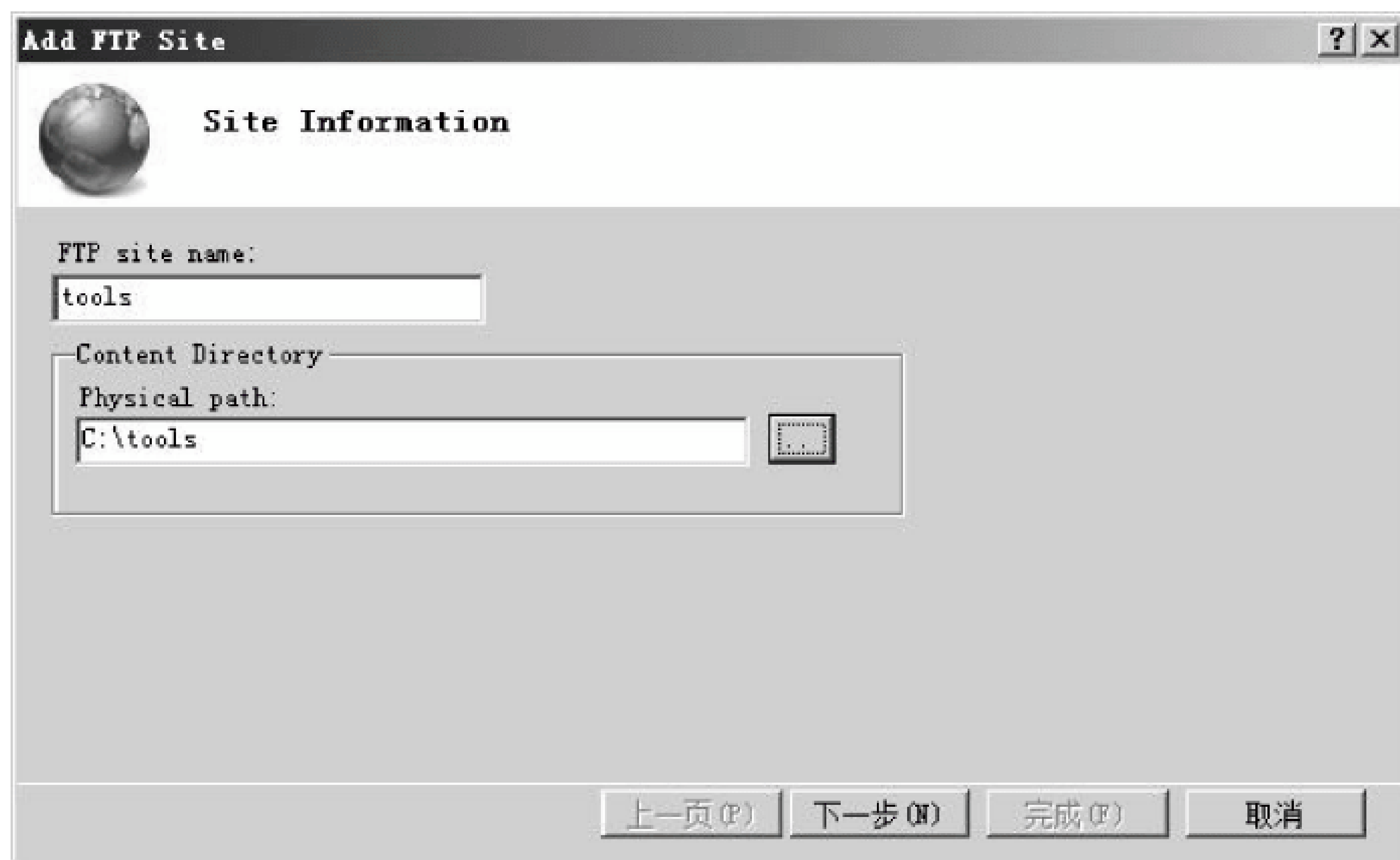



图 12-25 设置 FTP 站点信息

步骤 4：在打开的 Binding and SSL Settings 对话框中，选择 FTP 服务器绑定的 IP 地址，端口号使用默认的 21 号端口，选中“Enable Virtual Host Names:”，在虚拟主机框中输入 tools.lnpc.cn。在 SSL 选项中选择 No SSL。

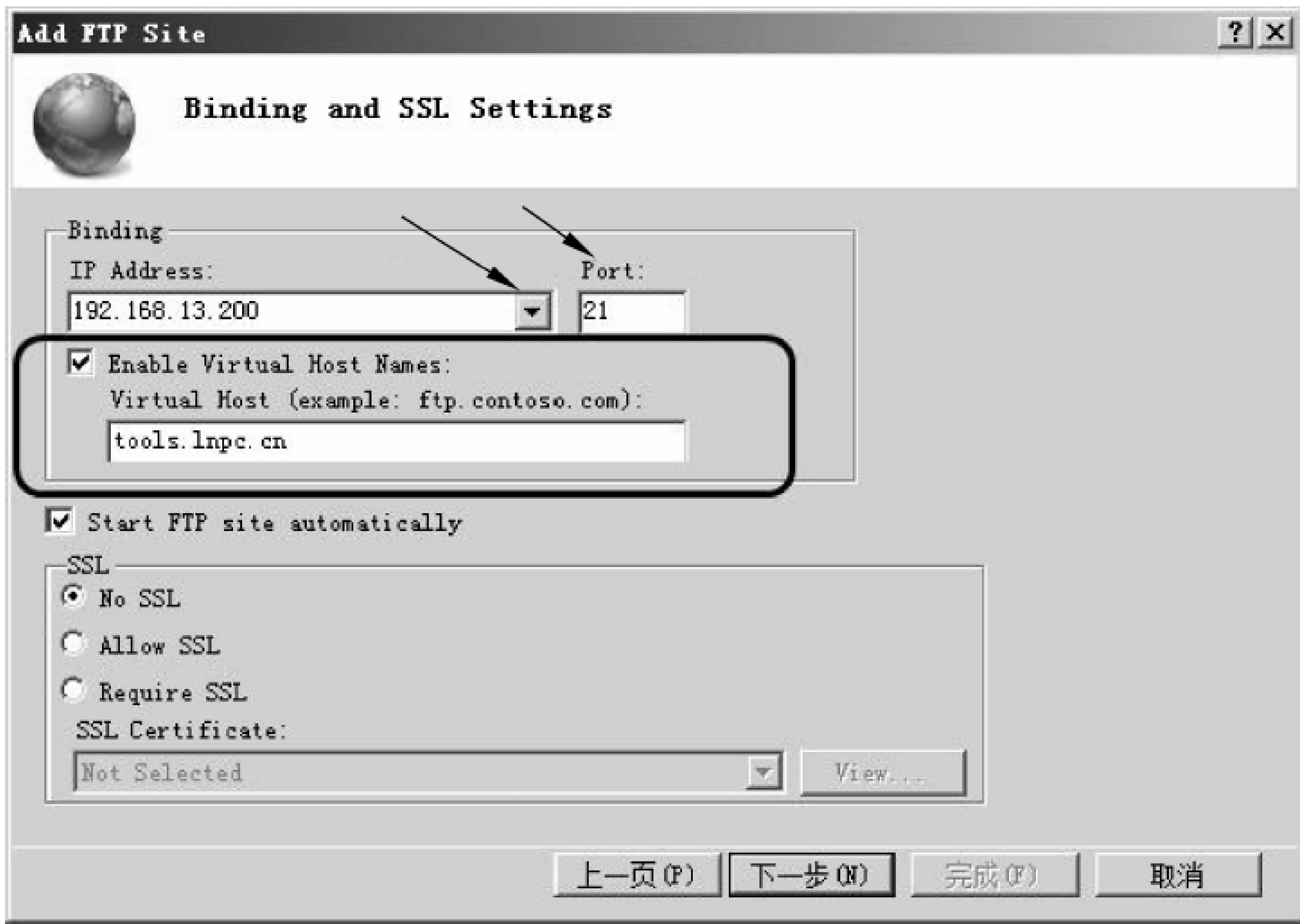



图 12-26　设置 FTP 站点的 IP 等信息

步骤 5：在打开的认证及授权对话框中，选择 Basic，允许存取下拉列表框中选择 Specified users，用户名填入 tom，读写权限都选中，如图 12-27 所示。




图 12-27　设置 FTP 站点的认证和授权信息

步骤 6：打开 FTP 客户端工具软件 FileZilla，如图 12-28 所示，在主机框中输入 tools.lnpc.cn，在用户名框中输入 tools.lnpc.cn|tom，再输入密码和端口号 21，单击“快速连接”，即可连接到 FTP 服务器了。

**注意**：用户名由两部分组成：tools.lnpc.cn 和 tom，中间用“|”连接。




图 12-28 FTP 客户端连接 FTP 服务器

步骤 7：再创建另一个 FTP 站点，步骤和 tools 站点相似，只是站点名为 film，主机名为 film.lnpc.cn。若为匿名用户的话，登录时的用户名应为 film.lnpc.cn|anonymous，密码为空。

# 12.4 FTP 站点的安全设置

## 12.4.1 通过 IP 限制连接

为了让 FTP 站点更安全，可以设置 FTP 站点允许、拒绝某个 IP 地址的主机登录 FTP 站点，或者是一群用户计算机。具体设置步骤如下。

步骤 1：在“Internet 信息服务(IIS)管理器”左侧，选择 FTP 站点 tools，双击中部窗格中的 FTP IPv4 Address and Domain Restriction，如图 12-29 所示。

步骤 2：窗口切换到图 12-30 所示状态，单击 Add Allow Entry→Add Deny Entry，添加一个 IP 地址，或者一个 IP 地址段。

## 12.4.2 FTP 站点用户的隔离

当用户登录到 FTP 站点后一般会被定向到站点的主目录，当然为了系统的安全，也可以把用户定向到用户自己的主目录，并且把它们限制在自己的主目录中，无法切换到其他用户的主目录，因此也就无法查看和修改其他用户的目录及其下的文件。

(1) 隔离用户各选项的含义如下。

如图 12-31 所示，双击 FTP User Isolation，打开如图 12-31 前图所示的界面。选择其中的选项，单击右侧“操作”窗格中的“应用”，保存更改。各选项的含义如下。




图 12-29　设置 FTP 站点的 IP 或域限制

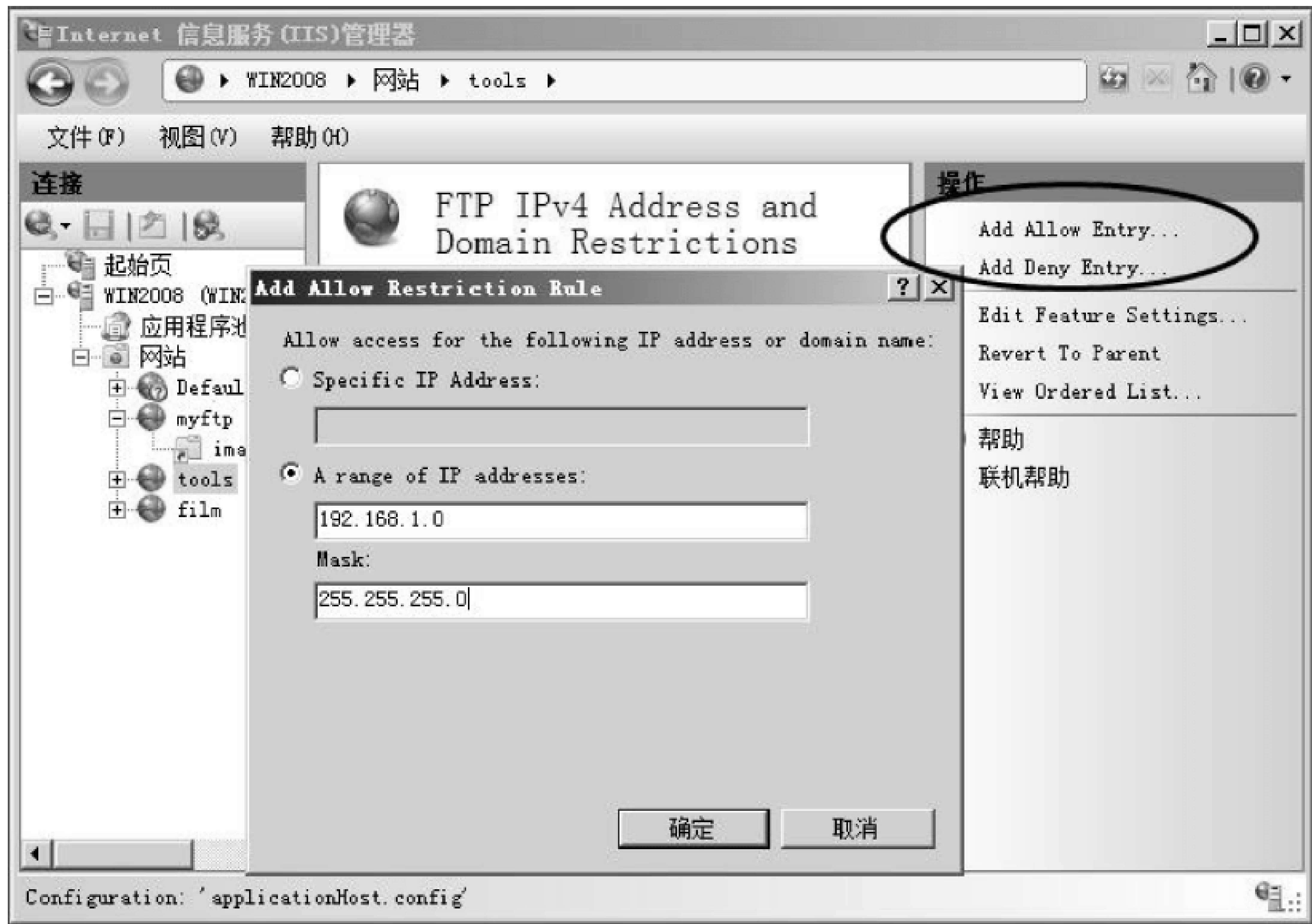



图 12-30　设置允许/拒绝的 IP 地址

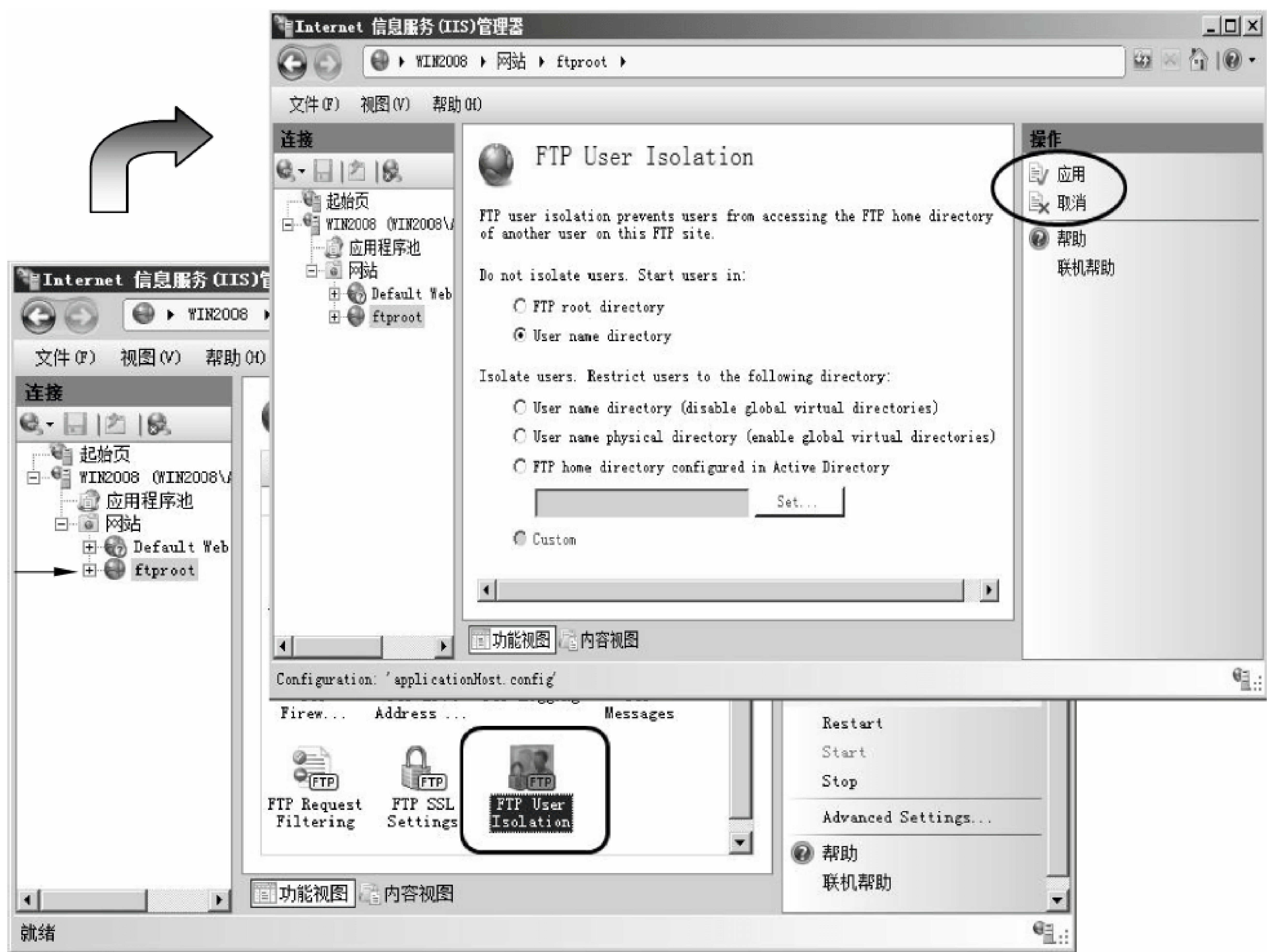



图 12-31 设置用户隔离

Do not isolate users. Start users in(不隔离用户)

• FTP root directory

用户被重定向到站点主目录,互不隔离,这是默认值。

• User name directory

用户拥有自己的主目录,不过互不隔离。用户可以切换到其他用户的目录,可以查看并修改其他用户的文件。

Isolate users. Restrict users to the following directory(隔离用户,严格限制在其主目录中)

• User name directory(disable global virtual directories)

在 FTP 主目录中建立与用户名同名的子目录,用户登录后便被定向于其主目录下,不能访问站点全局虚拟目录。

• User name physical directory (enable global virtual directories)

在 FTP 主目录中建立与用户名同名的子目录,用户登录后便被定向于其主目录下,可以访问站点全局虚拟目录。

• FTP home directory configured in Active Directory

用域账号连接访问 FTP 站点，必须在 Active Directory 中指定其主目录。

• Custom

自定义。

(2) 不隔离用户，但用户都有自己的主目录。

设置步骤如下所示。

步骤 1：新建用户。依次选择"开始"→"管理工具"→"计算机管理"→"系统工具"→"本地用户和组"→"用户"，新建用户 bob、lucy。

步骤 2：新建物理文件夹。在 C 盘下新建文件夹 C:\ftproot。在 C:\ftproot 下建立子文件夹 bob、lucy、default，C:\ftproot\bob 目录作为用户 bob 的主目录，在该目录下建立 bob.txt 文件；C:\ftproot\lucy 目录作为用户 lucy 的主目录，在该目录下建立 lucy.txt 文件；C:\ftproot\default 作为匿名用户登录后定向的默认目录，在该目录下建立 default.txt 文件。

步骤 3：新建 FTP 站点。在"Internet 信息服务(IIS)管理器"中新建一个 FTP 站点，站点名为 ftproot，物理路径为 C:\ftproot。网站绑定的 IP 是 192.168.13.200，端口号是 21，如图 12-32 所示。

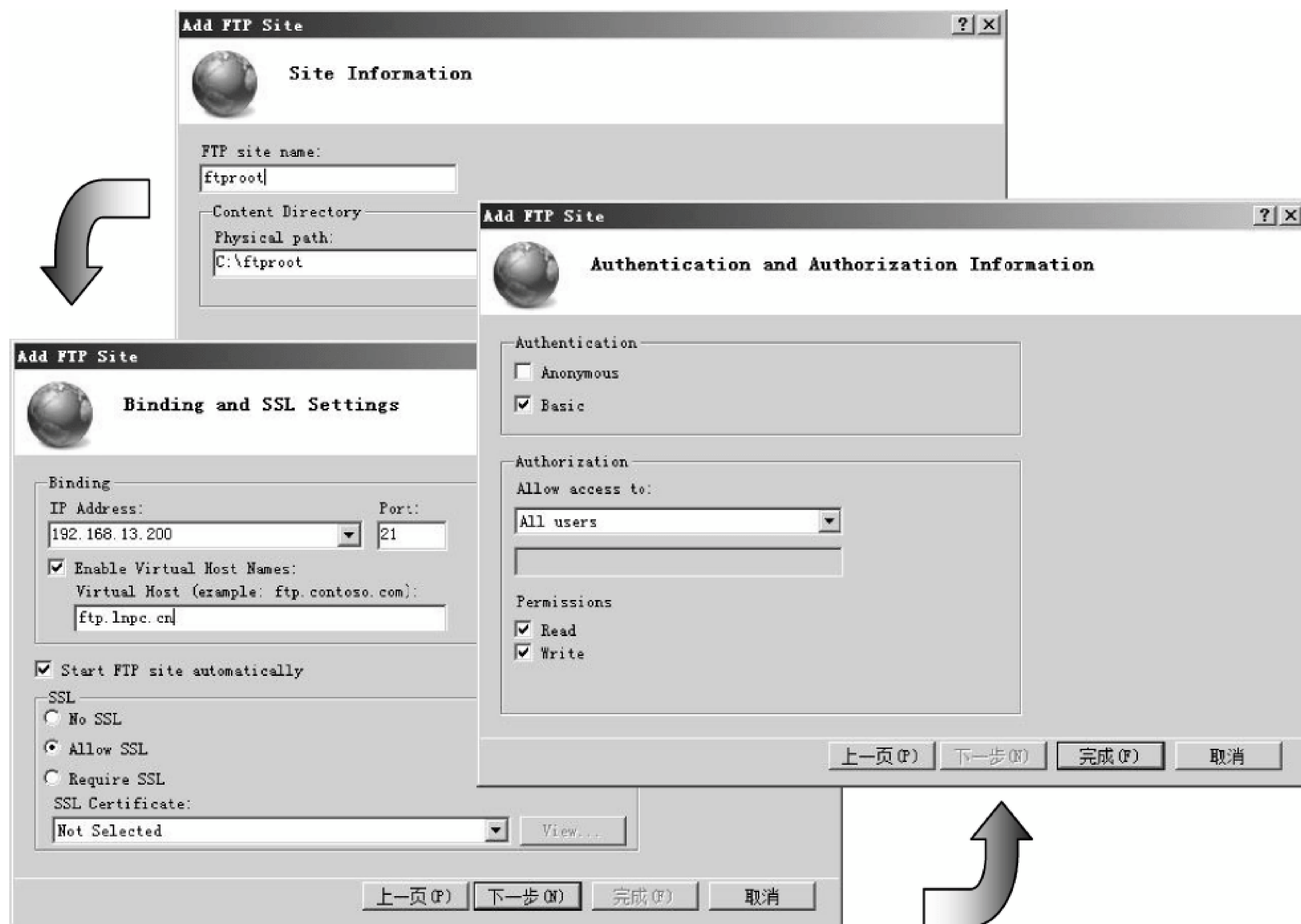



图 12-32　新建 FTP 站点

步骤 4：隔离用户。在“Internet 信息服务(IIS)管理器”左侧选择 ftproot 站点，双击 FTP User Isolation，打开用户隔离设置界面。如图 12-31 所示，选择 User name directory，然后，单击右侧窗格中的“应用”，保存设置。

用户隔离的测试：打开命令窗口，输入 ftp ftp.lnpc.cn 命令，输入用户名 ftp.lnpc.cn|bob、密码，登录成功后，执行 dir 命令，可以看到 bob.txt 文件，说明 bob 用户被定向到 C:\ftproot\bob 文件夹下。执行 cd ..\lucy 可以进入到 lucy 的主目录，即 C:\ftproot\lucy，如图 12-33 所示。

```
管理员: C:\Windows\system32\cmd.exe - ftp  ftp.lnpc.cn
C:\Users\Administrator>ftp ftp.lnpc.cn
连接到 ftp.lnpc.cn。
220 Microsoft FTP Service
用户(ftp.lnpc.cn:(none)): ftp.lnpc.cn|bob
331 Password required for ftp.lnpc.cn|bob.
密码:
230 User logged in.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
10-20-11  09:56PM                  0 bob.txt
226 Transfer complete.
ftp: 收到 48 字节，用时 0.02秒 2.40千字节/秒。
ftp> cd ..\lucy
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
10-20-11  09:57PM                 41 lucy.txt
226 Transfer complete.
ftp: 收到 49 字节，用时 0.02秒 2.45千字节/秒。
ftp> bye
221 Goodbye.
```

图 12-33 测试不隔离用户

(3) 隔离用户，有专属主目录，但不能访问全局虚拟目录。

用户拥有自己的专属目录，登录后会被定向到自己的专属目录，并被限制在该目录下，不能切换到其他用户的目录下，因此不能查看和修改其他用户的目录及其下的文件。

这里还是以 bob、lucy 为例。物理目录仍以 C:\ftproot 为 FTP 主目录，删除其下目录，新建 LocalUser 子目录，在 LocalUser 下新建与登录用户同名的目录，如 bob、lucy，新建 public 作为匿名用户的主目录。整个物理目录的结构如图 12-34 所示。bob 登录后会被定向到 C:\ftproot\LocalUser\bob 目录，lucy 登录后会定向到 C:\ftproot\LocalUser\lucy 目录，匿名用户 Anonymous 登录后会被定向到 C:\ftproot\LocalUser\public 目录。

FTP 站点设计：建立 FTP 站点 ftp，物理目录为 C:\ftproot，在其下建立虚拟目录 tools，在 lucy 目录下建立虚拟目录 image，复制一些文件到虚拟目录所在的物理目录。站点的逻辑结构如图 12-35 所示。

ftp 站点用户隔离模式选择 User name directory(disable global virtual directories)。认证模式若选择的是 Basic，在 Internet 信息服务(IIS)管理器中选择 ftp 站点后，双击 FTP

Authentication，选 Anonymous Authentication，再单击右侧的 Enable，把匿名用户设为 Enable 状态，匿名用户可以登录。




图 12-34　FTP 站点的物理目录的结构

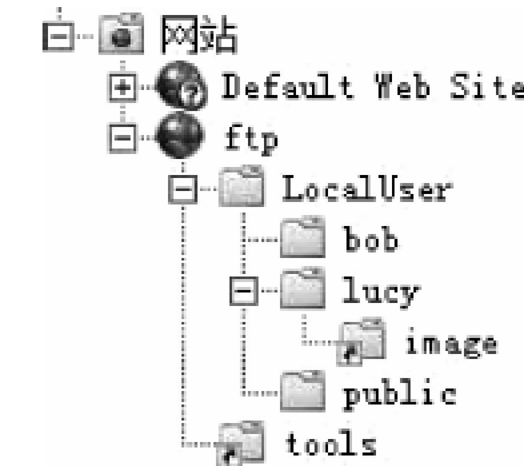



图 12-35　FTP 站点的逻辑结构

在命令行下，执行 ftp.exe 测试，执行结果如图 12-36 所示。




图 12-36　测试隔离用户

（4）隔离用户，有专属主目录，能访问全局虚拟目录。

设置这种隔离模式，只需在如图 12-31 所示的界面中单击 User name physical directory (enable global virtual directories)即可，其他设置和“隔离用户，但不能访问全局虚拟目录”模式一样。在这种模式下，用户被隔离在自己的专属目录下，可以访问全局虚拟目录，但不能访问专属目录中的虚拟目录。如图 12-35 所示的 FTP 站点中，Lucy 用户能访问 tools 虚拟目录，但不能访问他自己专属目录下的 image 虚拟目录。

### 12.4.3 限制最大连接数量

FTP 服务器进行文件传输时会占用较大的带宽，影响其他服务的正常运行，尤其是服务器中安装有 Web、DNS 等多个服务时，会因为 FTP 并发用户数量较多，而使其他服务中断或停止。因此有必要对最大连接数量进行限制。

在"Internet 信息服务(IIS)管理器"左侧选择 FTP 站点，在右侧"操作"窗格中选择 Advanced Settings，打开高级设置窗口，在这里可以设置最大连接数量，如图 12-37 所示。

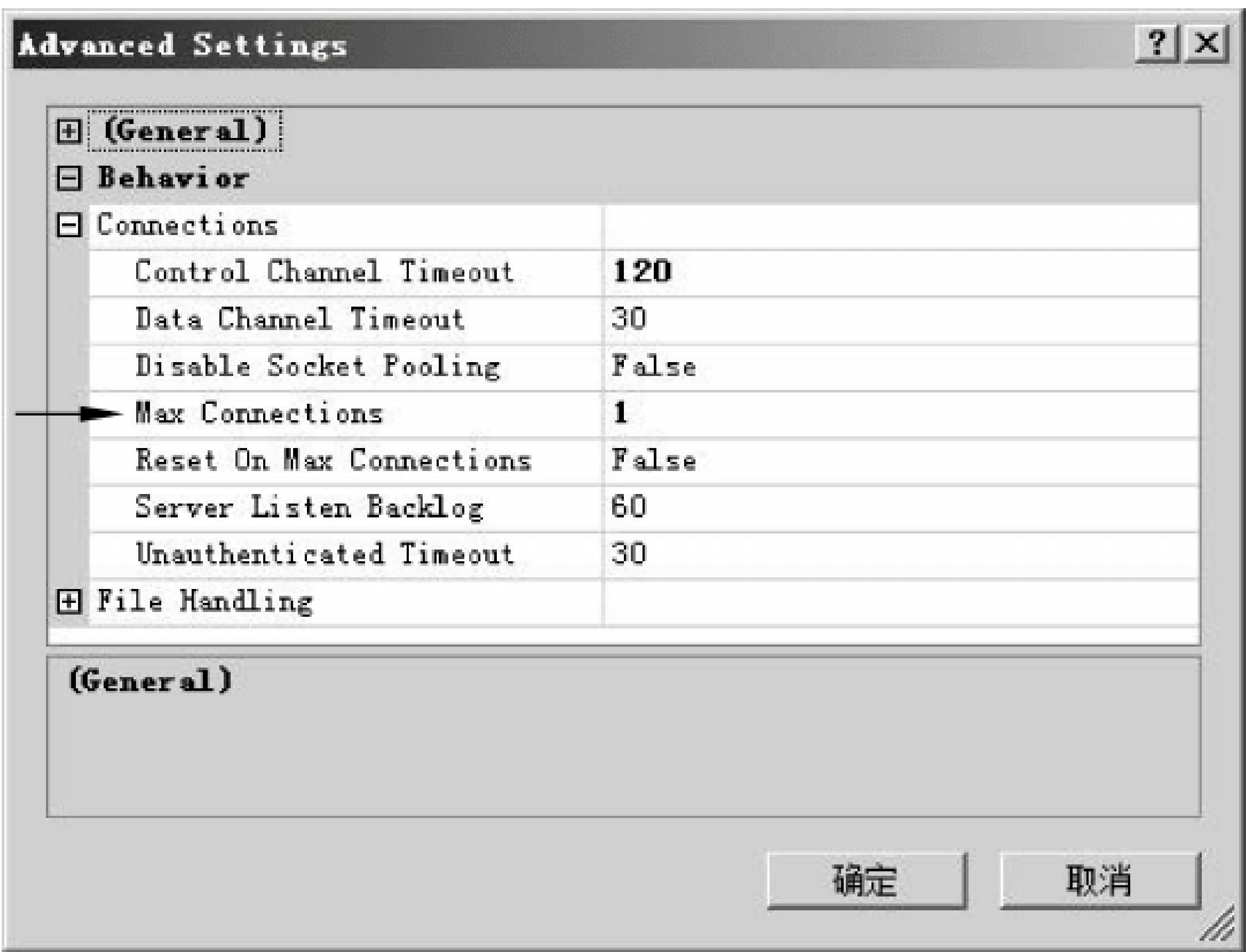



图 12-37 设置最大连接数

## 实验 17 FTP 服务器的配置

**1. 实验目标**

(1) 掌握 FTP 的工作原理。

(2) 掌握 Windows Server 2008 下 FTP 服务器的配置方法。

**2. 实验准备**

一台安装了 Windows Server 2008 的服务器，一台客户机；或者一台安装了虚拟机的性能较好的计算机

**3. 实验内容**

(1) 下载并安装 FTP 服务器软件。

(2) 架设一个用户可以匿名访问的 FTP 服务器。

(3) 架设一个和 Web 服务集成为一体的 FTP 站点。

(4) 通过 IP 地址、端口、域名三种方式架设多个 FTP 站点。

(5) 在系统中建立 usera、userb、userc 三个账号，建立 FTP 服务器，参照 12.4.2 节，练

习各种隔离用户的方法。

（6）在 Windows 客户机上通过多种方式测试 FTP 服务器的工作是否正常。

# 思考与练习

**一、填空题**

1. FTP 服务器的传输模式分为________模式和________模式。

2. FTP 采用两个独立的 TCP 通道，一个是用于传输命令的________，通常使用 21 号端口；另一个是用于传输数据的________，通常使用 20 号端口。

3. 可以设置的 FTP 信息包括________，________和________。

4. 可以通过________，________和________三种方式架设 FTP 虚拟主机。

**二、思考题**

1. 什么是 FTP？它的主要用途是什么？有何优缺点？

2. 简述 FTP 服务器的两种传输模式，理解两种模式对于防火墙的设置有何帮助。

3. 客户端通过几种方式、如何访问 FTP 服务器？

4. 为了防止恶意攻击，管理员应如何保护自己的 FTP 站点？

第 13 章

# 邮件服务器的配置与管理

## 13.1 邮件服务概述

电子邮件是 Internet 中应用比较广泛的一种网络服务,从 Internet 诞生开始它就受到用户的欢迎。与传统的通信手段相比,电子邮件服务具有以下优点。

(1) 速度快。发信人发出邮件后,在很短的时间内收信人就能收到邮件。

(2) 价格低廉。不用传递纸质邮件,只需要接入 Internet 的接入费用,随着网络的普及这个费用可以忽略不计。

(3) 操作简单方便。使用电子邮件客户端软件进行邮件的编辑、发送和接收,随着 Web 版邮件系统日渐增多,接发邮件更加方便快捷了。可以向多个接收者同时发送同一内容电子邮件,邮件可以添加附件,邮件内容可以包括文本、图像、音频、视频等多种形式。邮件系统还可以自动对邮件进行处理。

### 13.1.1 邮件相关的协议

SMTP(Simple Mail Transfer Protocol)即简单邮件传输协议,它是一组由源地址到目的地址传送邮件的规则,由它来控制信件的中转方式。SMTP 协议属于 TCP/IP 协议簇,它帮助每台计算机在发送或中转信件时找到下一个目的地,通过 SMTP 协议,我们就可以把 E-mail 从我们的计算机(即客户端)发送到收信人的服务器上。在发送邮件的过程中必须依赖于 DNS,把邮件服务器的域名解析为 IP 地址,客户端与收信端服务器建立连接并接收信件。SMTP 使用 TCP 的 25 号端口,在传输的邮件数据流中既包括邮件内容也包括 SMTP 命令。

POP3(Post Office Protocol 3)即邮局协议的第 3 个版本,它规定了怎样将个人计算机连接到 Internet 的邮件服务器并下载电子邮件的协议标准。邮局协议要检查用户名和口令,然后将用户的邮件从邮件服务器下载到客户端,同时删除保存在邮件服务器上的邮件。POP3 协议在服务器端使用 110 端口。

IMAP4(Internet Message Access Protocol)即互联网消息访问协议,可以替代 POP 协议,除了提供 POP 的功能外,还新增加了一些功能。用户使用 IMAP 可以远程维护邮件服务器上的邮箱,在服务器上收发电子邮件,可在邮件服务器上建任意层次的文件夹,可以灵活地在文件夹之间移动邮件。IMAP 提供了选择性地下载附件的服务,比如邮件有三个附件,用户可以

下载其中的一个。用户的邮件可以长期保存在服务器上，用户可以在任意时间地点登录阅读邮件。IMAP4 协议在服务器端监听 143 号端口，目前许多邮件服务器都支持 IMAP4 协议。

### 13.1.2　邮件系统的组成

电子邮件系统主要由两部分组成：邮件服务器和邮件客户端。

**1. 邮件服务器**

邮件服务器实际上就是安装有邮件服务软件的服务器，称其为邮件传输代理（Mail Transfer Agent，MTA），MTA 负责邮件的存储与转发，将邮件在服务器之间进行传输和缓存。MTA 根据邮件的目的地址把邮件传输到目的服务器或经过中转服务器传到目的服务器。MTA 将接到的邮件进行缓冲，根据邮件地址选择下一个邮件应该转往的 MTA，这个 MTA 可能是目的服务器，也可能是中转服务器。

MTA 接收和传递由客户端传递过来的邮件，缓冲和维护邮件队列。MTA 接收来自其他 MTA 服务器的邮件，将邮件缓冲并根据邮件地址选择传递到下一个 MTA，如果邮件的接收用户是本地用户，则把邮件直接放到用户的邮箱中。

**2. 邮件客户端**

发送者发送邮件和接收者接收邮件用的是自己的个人计算机，因此称其为邮件客户端。客户端可以向服务器发送邮件或从服务器接收邮件。发送邮件时客户端使用 SMTP 协议把邮件推送给邮件服务器；收信时客户端使用 POP 或 IMAP 协议把邮件下拉到客户端计算机。用户可以在客户机上对邮件进行编写、阅读、回复、转发、删除操作。

## 13.2　通过邮件服务器传送电子邮件

### 13.2.1　TurboMail 邮件服务软件的安装与配置

现在有许多电子邮件服务器软件，其中包括微软的 Exchange Server、MDaemon 以及国内的 FoxMail、U-mail、TurboMail 等，其中 TurboMail 用 Java 开发，可以跨平台使用，本章使用 TurboMail 作为示例软件讲解邮件服务器的架设。

步骤 1：下载安装软件。到 TurboMail 的官方网站 http://www.turbomail.org 的下载中心选择适合使用平台的版本。这里我们使用 Windows 平台版本。下载文件为 turbomail_win_430.zip，解压后双击 turbomail_win_430.exe 即可安装。安装完成系统重新启动后，在后台运行着 TurboMail Server 服务和 TurboMail_Web（Tomcat6）服务。

步骤 2：登录邮件服务器。在服务器上打开浏览器，输入 http://127.0.0.1:8080，即可打开登录界面。单击“管理员入口”按钮，打开管理员入口界面，管理员默认的用户名为 postmaster，密码为空，如图 13-1 所示。单击“登录”按钮，进入系统设置界面。

步骤 3：添加域。单击界面左边的“域管理”，在窗口右边选“普通属性”，在“域”文本框中输入域名 lnpc.cn，单击页面右下方的“保存”按钮保存设置，如图 13-2 所示。




图 13-1　TurboMail 的 Web 登录界面

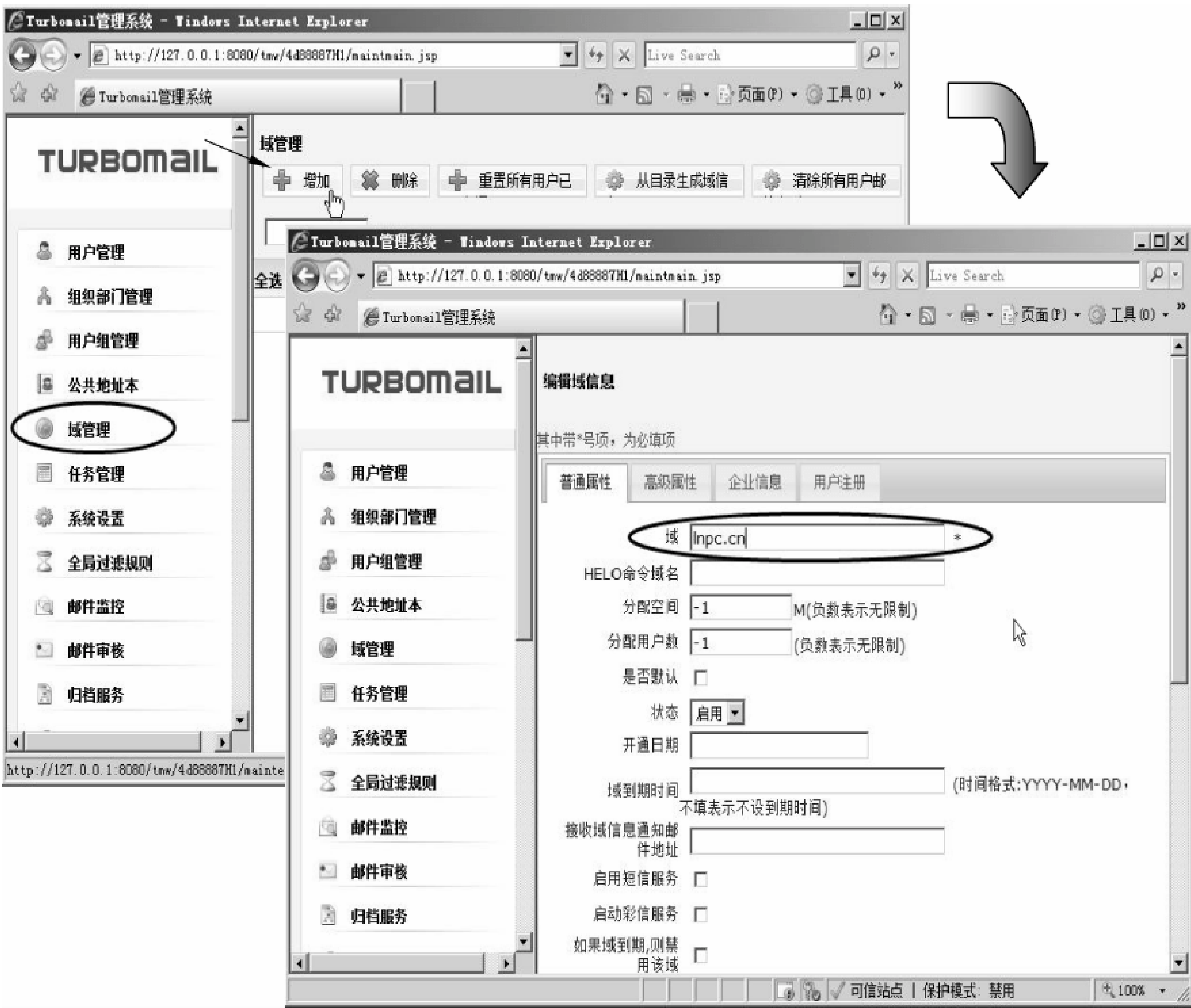



图 13-2　增加域

步骤 4：增加用户。单击浏览器界面左侧的“用户管理”打开用户管理界面。单击右侧的“增加”按钮打开“编辑用户”界面，在“一般属性”选项卡中，输入用户名“user1”，昵称“张三”，密码“123456”，单击右侧下部的“保存”按钮。同样方法，增加用户“user2”。单击左侧“退出”退出系统的设置，如图 13-3 所示。

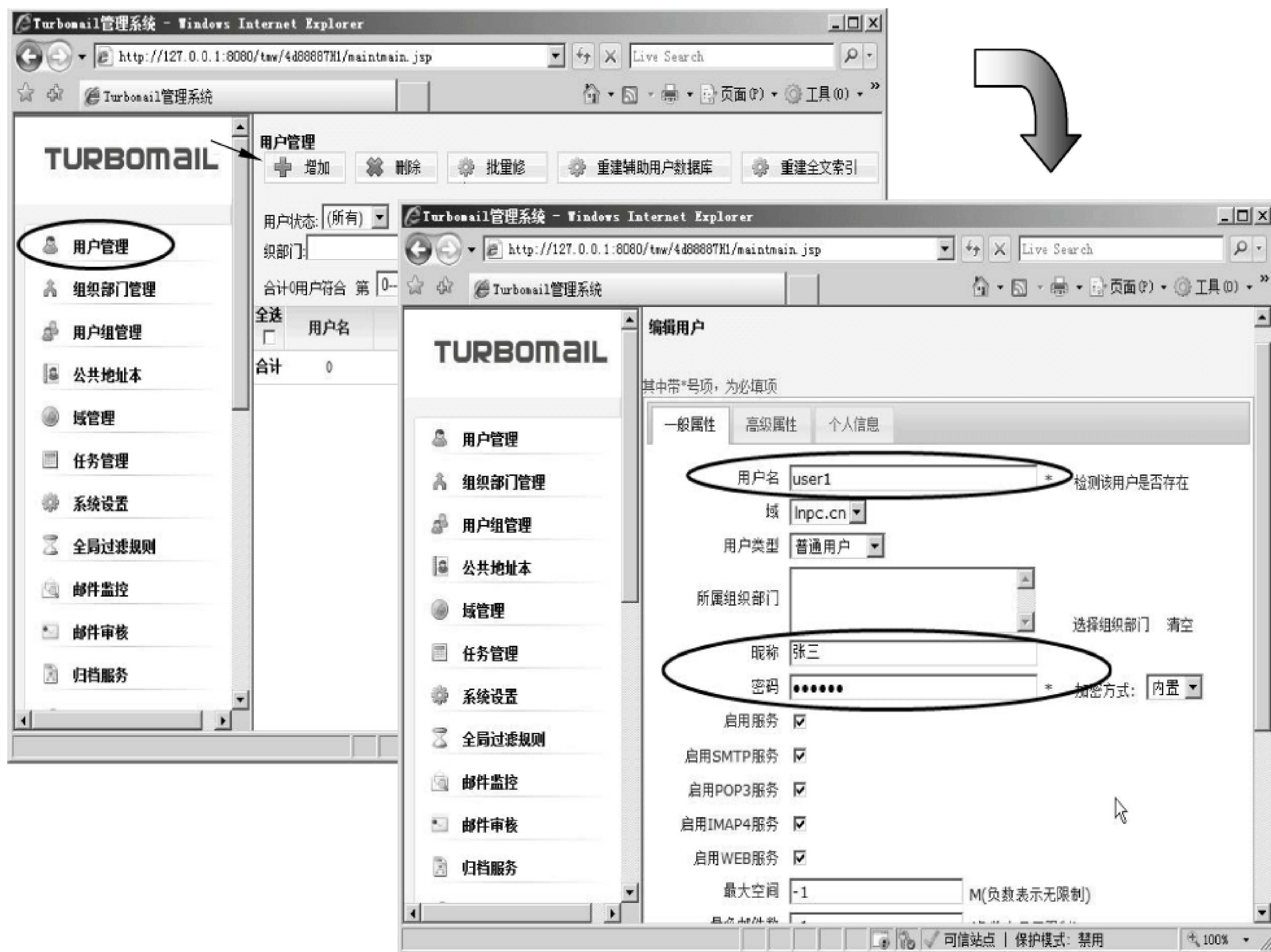



图 13-3　增加用户

步骤 5：增加 A 记录 mail. lnpc. cn。依次打开“开始”→“管理工具”→DNS，在“DNS 管理器”左侧的“正向查找区域”下的 lnpc. cn 上右击，选择“新建主机(A 或 AAAA)”，在打开的“新建主机”对话框中输入名称“mail”，IP 地址为“192. 168. 13. 200”，即邮件服务器的 IP 地址。勾选“创建相关的指针(PTR)记录”，如图 13-4 所示。

步骤 6：新建 MX 记录。邮件交换(Mail Exchange，MX)记录用于指出某个 DNS 区域中的邮件服务器的主机名(A 记录)，它相当于一个指针，因此在创建 MX 记录之前，你必须已经为邮件服务器创建了 A 记录。在主机或子域栏输入邮件域的域名，留空则代表父区域。邮件域代表“@”后的域名后缀，例如“@lnpc. cn”的邮件域是“lnpc. cn”，而“@mail. lnpc. cn”的邮件域是“mail. lnpc. cn”。我们针对邮件域 lnpc. cn 创建 MX 记录，因此留空(代表父域名 lnpc. cn)，用户 user1 的邮箱地址是 user1@lnpc. cn；如果你要针对邮件域 mail. lnpc. cn 创建 MX 记录，则“主机或子域”输入 mail，在下面的完全合格的域名(Fully

Qualified Domain Name,FQDN)文本框会显示出你当前的邮件域域名,user1 的邮箱地址是 user1@mail.lnpc.cn,如图 13-5 所示。




图 13-4 新建主机 mail 的 A 记录

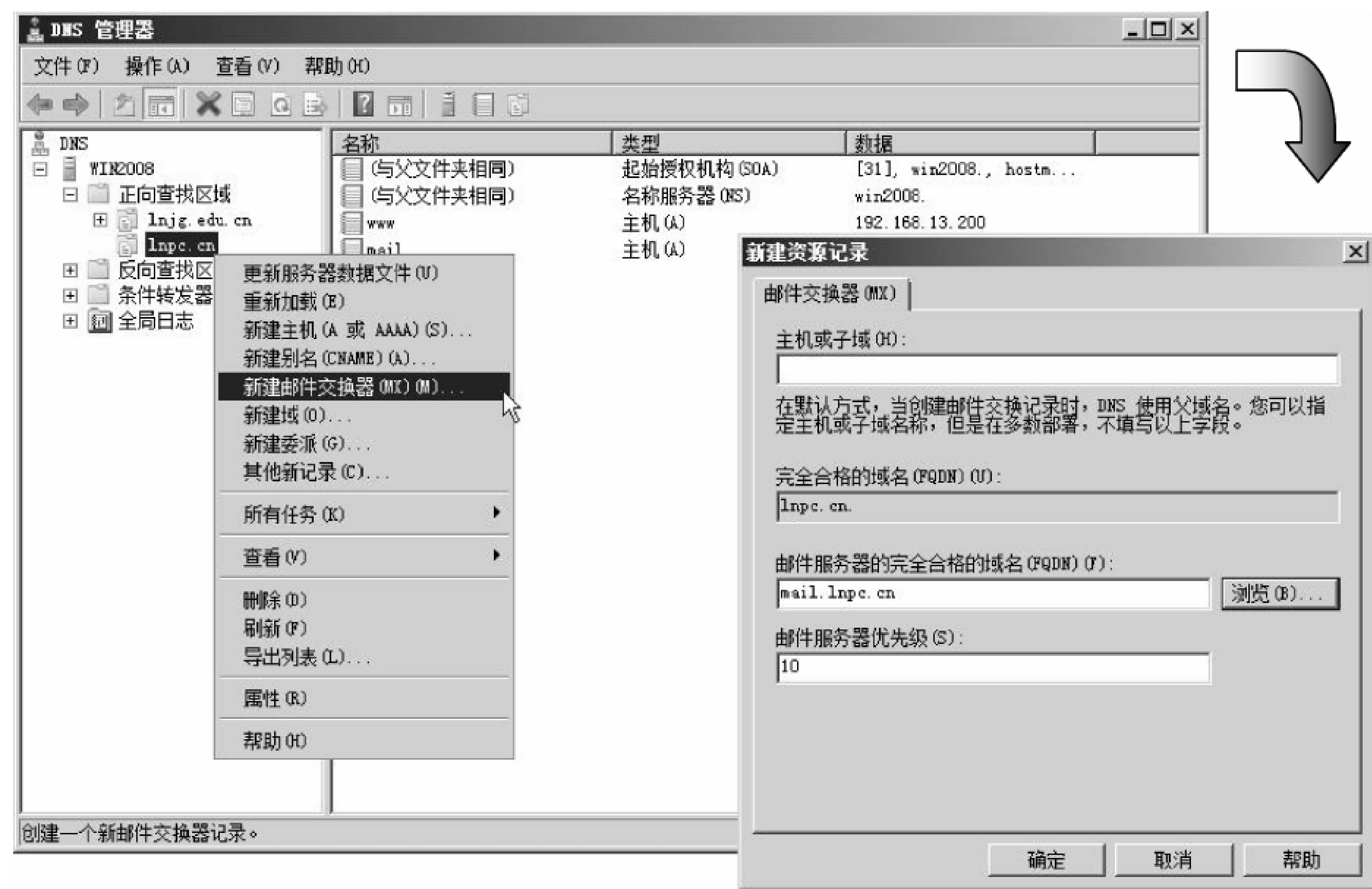



图 13-5 新建 MX 记录

步骤 7：设置邮件服务器的 DNS 地址。以邮件服务器管理员身份登录，选择左边窗格的“系统设置”，单击“SMTP 服务”。把右边新打开的窗格往下拉，找到“DNS 服务”文本框，输入 DNS 服务器的 IP 地址 192.168.13.200，单击“保存”按钮，然后退出系统，如图 13-6 所示。

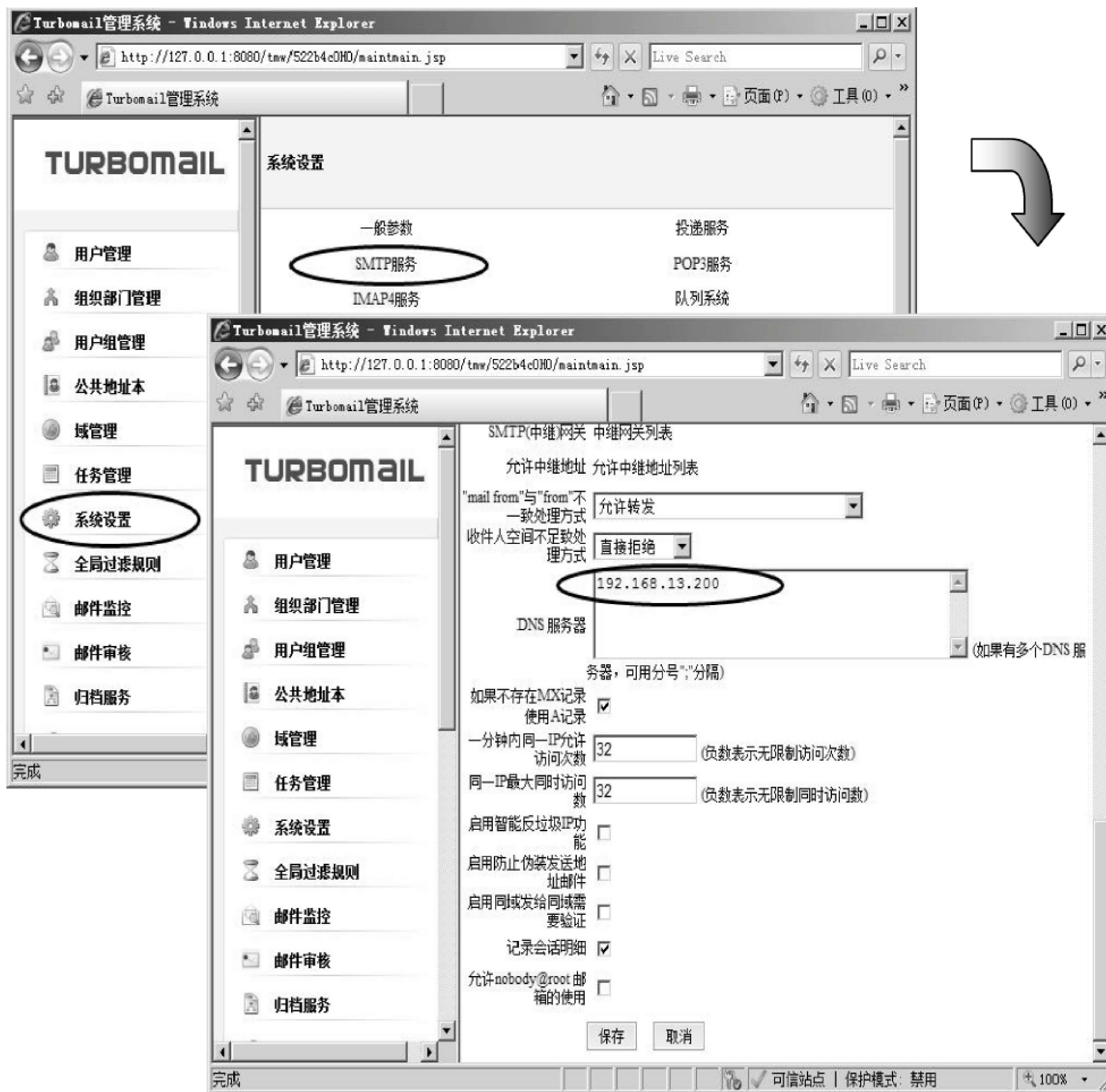



图 13-6　设置邮件服务器的 DNS 地址

步骤 8：通过 Web 方式登录。在客户端打开浏览器，输入 http://mail.lnpc.cn:8080/地址，输入用户名 user1，密码 123456，单击“登录”进入邮件系统。就可以给 user2 用户发邮件了。

## 13.2.2 客户端 Outlook Express 的设置

步骤 1：打开客户端 Windows 自带的 Outlook Express，选择菜单“工具”→“账户”，打开“Internet 账户”窗口，单击“添加”→“邮件”，如图 13-7 所示。




图 13-7 添加邮件帐户

步骤 2：设置用户信息。在打开的“Internet 连接向导”中，输入用户名 user1，电子邮件地址 user1@lnpc.cn，接收和发送邮件服务器的地址 mail.lnpc.cn，如图 13-8 所示。

步骤 3：在 Outlook Express 中选择菜单“工具”→“账户”打开“Internet 账户”窗口，选择列表中的“mail.lnpc.cn”，单击“属性”按钮，打开“mail.lnpc.cn 属性”对话框，选择“服务器”选项卡，选中“我的服务器要求身份验证”，单击“确定”按钮，如图 13-9 所示。设置完成后在 Outlook Express 中就可以使用 user1 账号收发邮件了。

## 13.2.3 邮件服务的测试

### 1. 邮件服务器内用户互发邮件

在新建的邮件服务器内新建域 lnpc.cn，新建用户 user1 和 user2 两个用户。他们的邮箱地址分别是 user1@lnpc.cn 和 user2@lnpc.cn。user1 通过 Web 方式登录，user2 通过邮件客户端 Outlook Express 登录，互相发送邮件。这种模式下邮件服务和域名服务可以放




图 13-8　设置邮件用户信息

在同一台服务器上，以节省设备资源，如图 13-10 所示。

**2. 不同域的用户互发邮件**

本测试通过在局域网中模拟建立两个不同域 lnpc.cn 和 lnjg.edu.cn。

(1) 邮件服务器的安装与设置。lnpc.cn 域中建立有邮件服务器 mail.lnpc.cn；lnjg.edu.cn 域中建立有 mail.lnjg.edu.cn。设置两个邮件服务器的 DNS 服务器的 IP 地址。

(2) 为简化域名服务器的设置，仅建立一个域名服务器，域名服务器内建立两个正向解析域 lnpc.cn 和 lnjg.edu.cn，在 lnpc.cn 域内建立 A 记录 mail.lnpc.cn，MX 记录指向 mail.lnpc.cn；在 lnjg.edu.cn 域内建立 A 记录 mail.lnjg.edu.cn，MX 记录指向 mail.lnjg.edu.cn。

(3) 用户的设置。在 mail.lnpc.cn 服务器内建立一个用户 user1，其邮箱地址是 user1@lnpc.cn；在 mail.lnjg.edu.cn 内建立用户 user2，其邮箱地址是 user2@lnjg.edu.cn，两个用户互相发送邮件，如图 13-11 所示。




图 13-9 设置账户属性

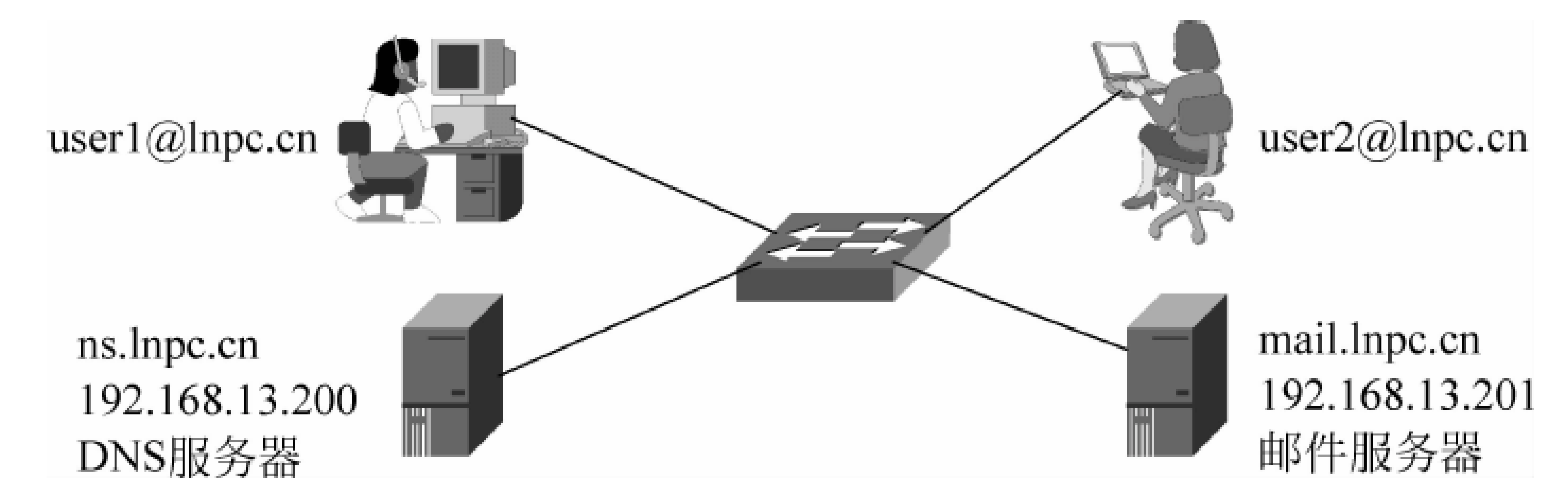



图 13-10 单邮件服务器用户之间互发邮件

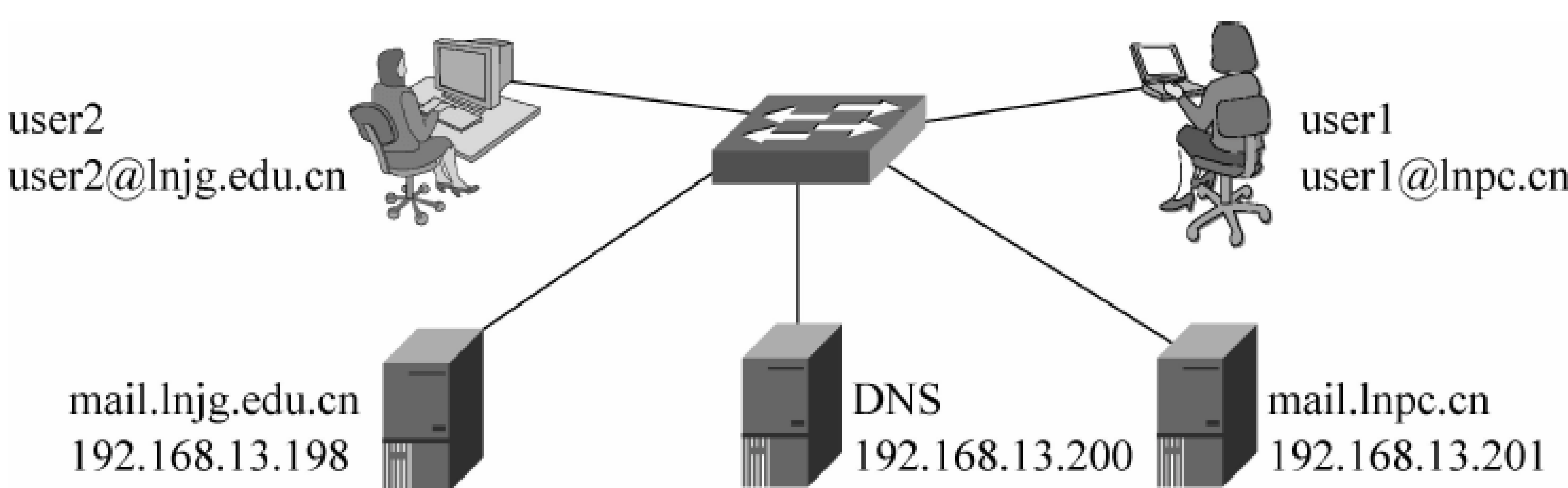



图 13-11 模拟不同域间用户互发邮件

# 13.3　SMTP 中继服务器的安装与设置

在发送邮件时经常会有发送失败的情况，失败的原因主要有以下几方面。

（1）发送方目前所获取的 IP 地址可能因下列原因被反垃圾组织列入黑名单：

- 局域网中某一电脑曾经中过蠕虫病毒，发送大量病毒/垃圾邮件，导致发送方出口 IP 被列入黑名单。
- 发送方获取 IP 前曾经被垃圾制造者利用，被列入黑名单。
- 发送方获取的 IP 段为 ADSL 动态地址。

（2）发送方目前 IP 未申请到反向解析。

（3）对方管理员因为反垃圾屏蔽了发送方的邮件。

（4）因为线路故障，发送方出口链路连接某些对方服务器速度缓慢或者彻底中断。

这时就需要 SMTP 中继服务器来转发邮件了。中继转发就是通过别的邮件服务器（中继服务器）将源邮件系统的邮件转发到目标地址。也就是说，当您的邮件服务器无法正常发信时，通过这个中继服务器转发邮件，相当于有了一条备用邮件发送通道。

如图 13-12 所示，SMTP 服务在邮件系统中起到中继的作用，当 user1 发送邮件时，它首先把邮件发送到 mail. lnpc. cn 服务器，mail. lnpc. cn 服务器把收到的邮件发送到 SMTP 中继服务器，中继服务器再把邮件发送到 mail. lnjg. edu. cn 服务器，jg1 用户到 mail. lnjg. edu. cn 服务器上把邮件取回到客户机上。

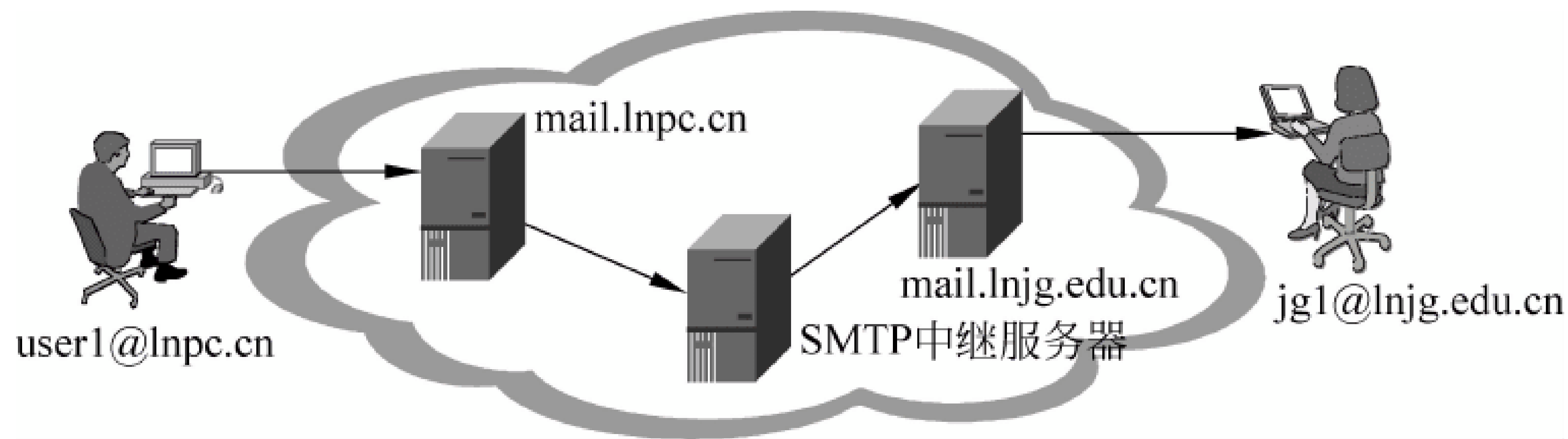



图 13-12　通过中继服务器的邮件发送过程

## 13.3.1　SMTP 服务器的安装

步骤 1：依次选择"开始"→"管理工具"→"服务器管理器"，在服务器管理器窗口的左侧窗格中选择"功能"，在右边窗格中单击"添加功能"，如图 13-13 所示。

步骤 2：打开"添加功能向导"对话框，选择"SMTP 服务器"，在弹出的"添加功能向导"对话框中单击"添加必需的角色服务"按钮，一直单击"下一步"按钮，如图 13-14 所示。

步骤 3：在"确认安装选择"对话框中，单击"安装"。

步骤 4：在"安装结果"对话框中，单击"关闭"按钮，结束安装过程。




图 13-13　添加邮件服务功能

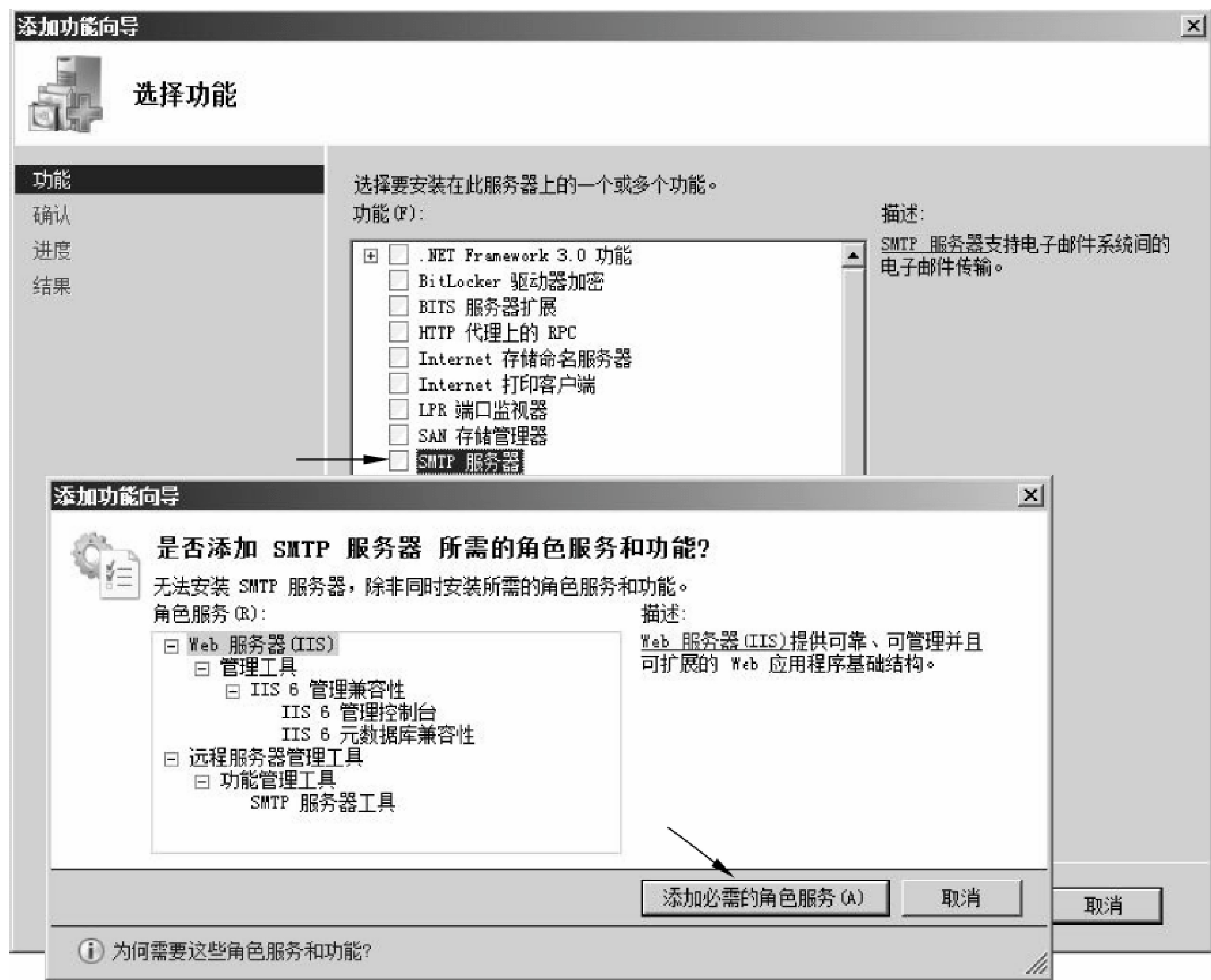



图 13-14　选择 SMTP 服务器

## 13.3.2　启动/停止 SMTP 服务

### 1. 在 IIS 6.0 中启动/停止 SMTP 服务

依次选择"开始"→"管理工具"→"Internet 信息服务(IIS)6.0 管理器",在打开的"Internet 信息服务(IIS)6.0 管理器"窗口中右击"SMTP Virtual Server ＃1"选择弹出菜单中的"启动"、"停止"或"暂停"菜单项。也可以单击工具栏上的三个按钮,如图 13-15 所示。

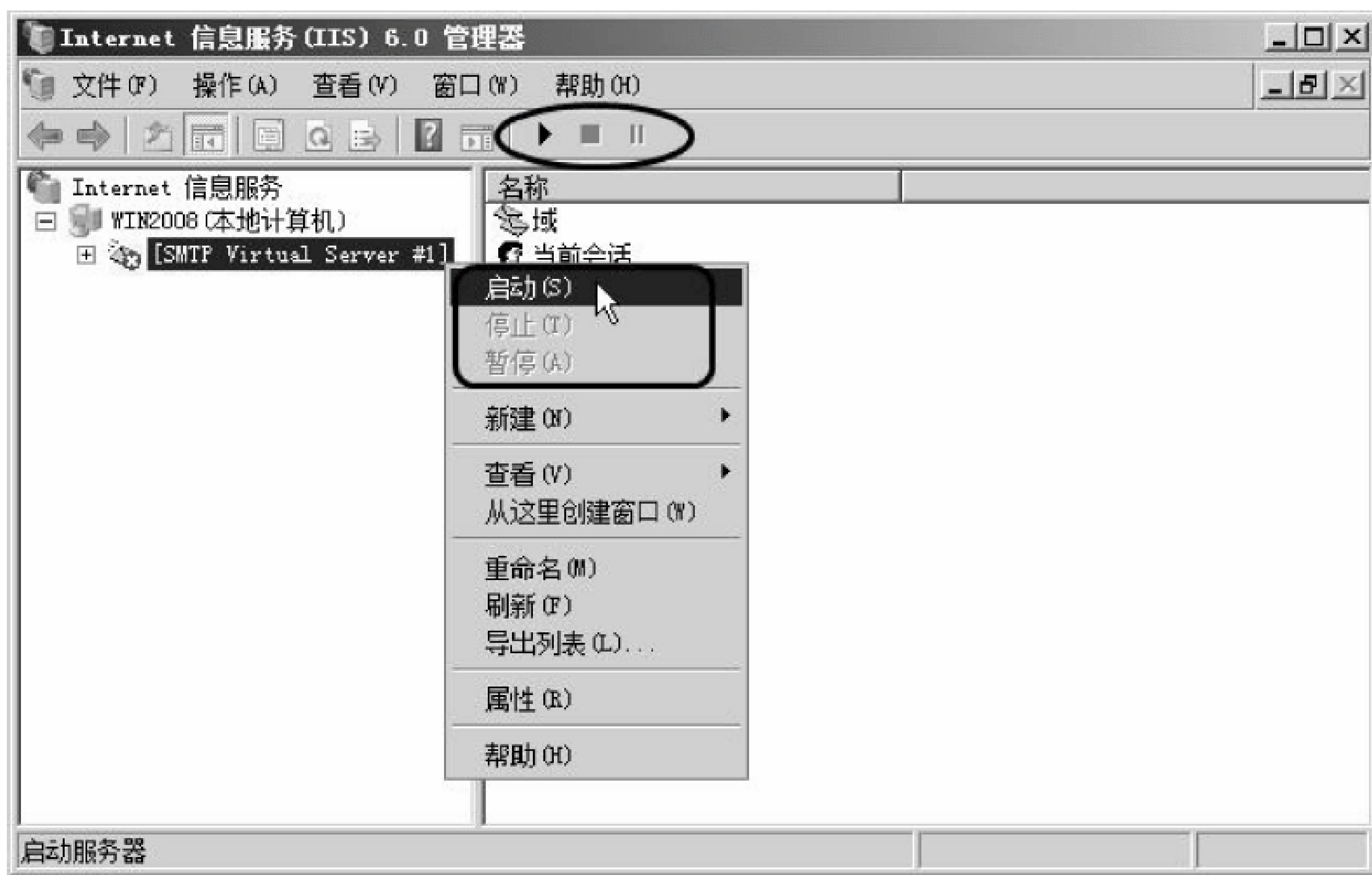



图 13-15　在 IIS 管理器中启动/停止 SMTP 服务

### 2. 在服务窗口中启动/停止 SMTP 服务

依次选择"开始"→"管理工具"→"服务",打开"服务管理窗口"。右击 Simple Mail Transfer Protocol(SMTP)服务项,选择弹出菜单中的"启动"、"停止"、"暂停"或"重新启动";或单击工具栏上的四个按钮;也可以单击窗口中部的文字,如图 13-16 所示。

## 13.3.3　SMTP 服务器的 IP 与端口的设置

如果 Windows Server 2008 绑定了多个 IP 地址,用户可以选择提供 SMTP 服务的 IP 地址,设置后的 SMTP 服务器只接受此 IP 地址传递过来的电子邮件。

端口是用来识别 TCP/UDP 协议的,默认的 SMTP 服务的端口号是 25。如果在一台 Windows Server 2008 服务器中架多台 SMTP 服务器,这些服务器在 IP 地址和端口号上必须不能完全相同。

若要改变 SMTP 服务器的 IP 地址或端口号,在"Internet 信息服务(IIS)6.0 管理器"中右击"SMTP Virtual Server ＃1",选择"属性"选项,打开"[SMTP Virtual Server ＃1]属性"窗口。选择"常规"选项卡,在"IP 地址"下拉列表框中选择 SMTP 服务器的 IP 地址,如图 13-17 所示。

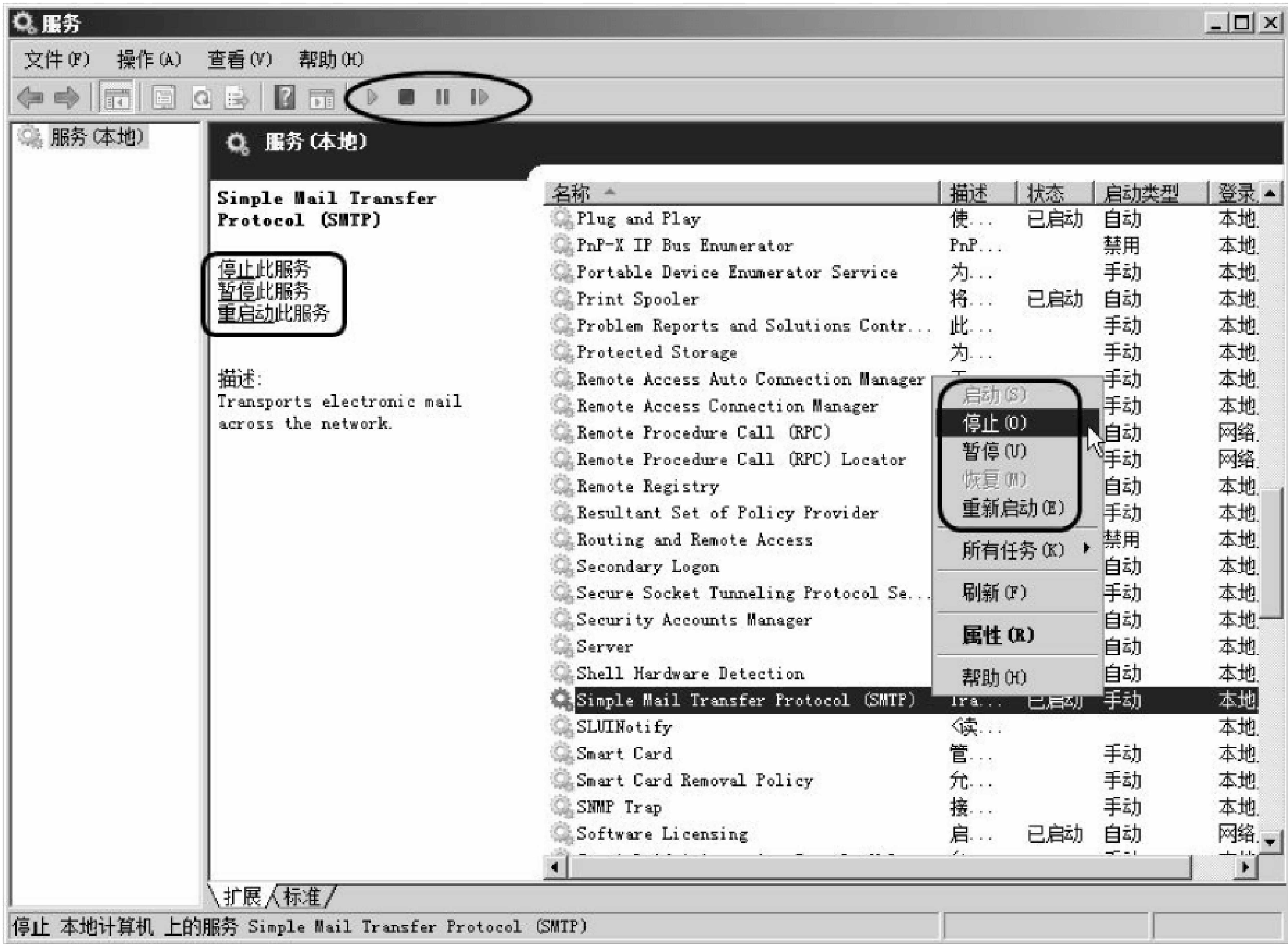



图 13-16　在服务窗口中启动/停止 SMTP 服务




图 13-17　修改 SMTP 服务器的 IP 地址

若要设置端口，单击“[SMTP Virtual Server ＃1]属性”窗口中的“常规”选项卡中的“高级”按钮，打开“高级”对话框，单击“编辑”按钮，在打开的“标识”对话框中，选择 IP 地址，输入端口号，如图 13-18 所示。




图 13-18　设置 SMTP 服务器的 IP 与端口

## 13.3.4　新建 SMTP 虚拟服务器

步骤 1：在打开的“Internet 信息服务(IIS)6.0 管理器”窗口中右击“SMTP Virtual Server ＃1”，选择弹出菜单“新建”→“虚拟服务器”，如图 13-19 所示。




图 13-19　新建 SMTP 虚拟服务器

步骤 2：进入“新建 SMTP 虚拟服务器向导”分别输入服务器的名称，选择服务器 IP 地址，选择服务器的主目录以及服务器的默认域，如图 13-20 所示。




图 13-20 设置虚拟 SMTP 服务器

### 13.3.5 连入连接的身份验证设置

用户或远程 SMTP 服务器连入服务器时，可以设置他们的身份验证方式，身份验证方式的设置步骤如下。

右击 SMTP 服务器，选择弹出菜单“属性”，在 SMTP 服务器“属性”窗口中选择“访问”选项卡，单击“身份验证”按钮，弹出“身份验证”窗口，如图 13-21 所示。

- 匿名访问：用户或其他 SMTP 服务器不需要用户名和密码就可以连接该 SMTP 服务器。
- 基本身份验证：用户或其他 SMTP 服务器需要提供用户名和密码才连接该服务器，不过密码是以不加密的明文方式发送的。因此，选择此选项后，最好同时选择“要求 TLS 加密”。
- 集成 Windows 身份验证：用户或其他 SMTP 服务器需要使用用户名和密码来连接该 SMTP 服务器，密码是加密的。

若用户以匿名方式连入 SMTP 服务器，该 SMTP 服务器仅接受传入的服务器，而不能外传邮件。

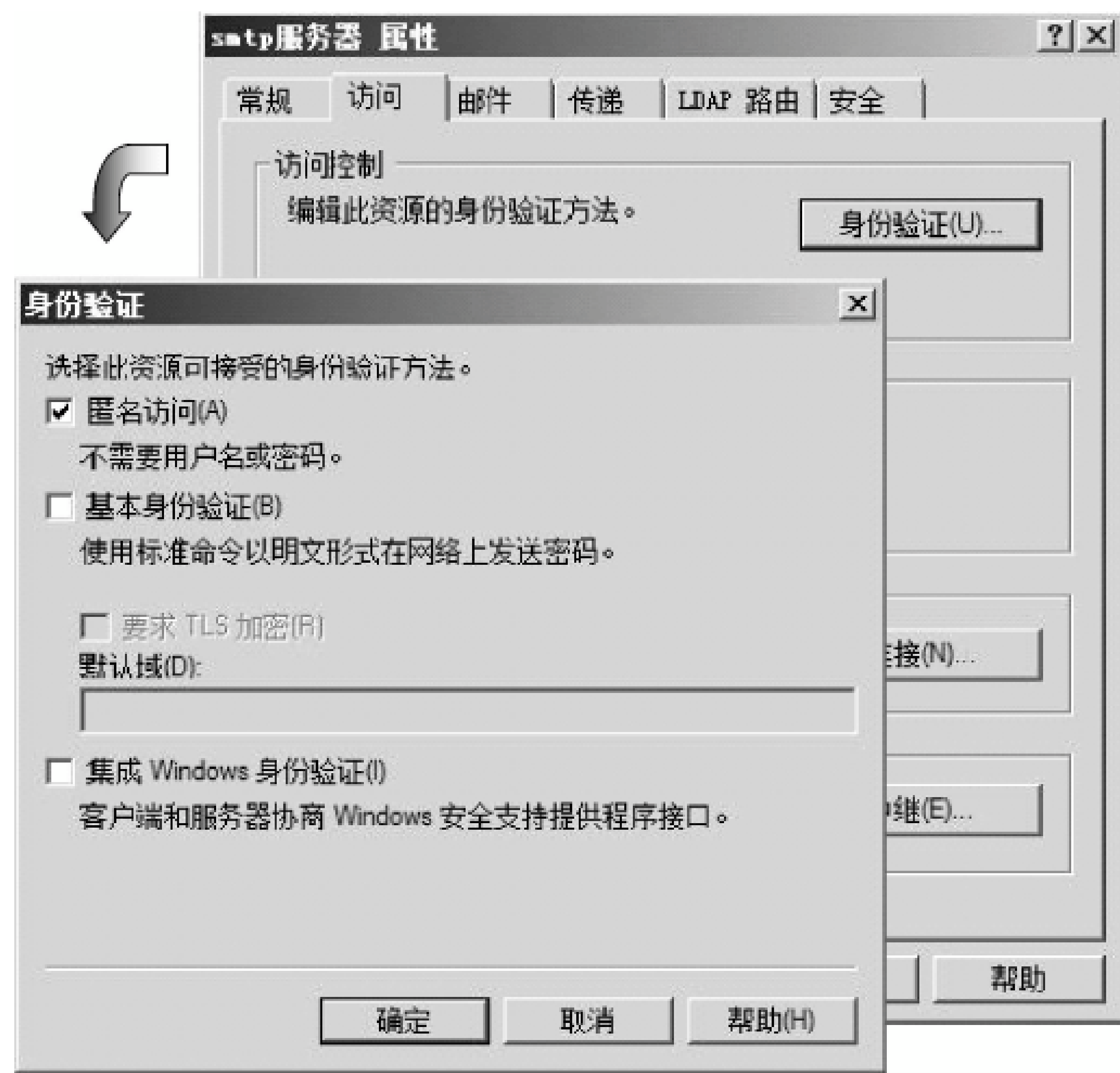



图 13-21　连入连接验证设置

## 13.3.6　出站连接的身份验证设置

当你的 SMTP 服务器连接到其他 SMTP 服务器时，需要按照对方的验证要求选择适当的验证要求。验证设置方法如下所示。

在 SMTP 服务器上右击，选择“属性”弹出菜单项，在“属性”对话框中选择“传递”选项卡。选择“出站安全”按钮，打开“出站安全”对话框，出站安全身份验证方式也是有三种方式，可参照连入连接验证方式，如图 13-22 所示。

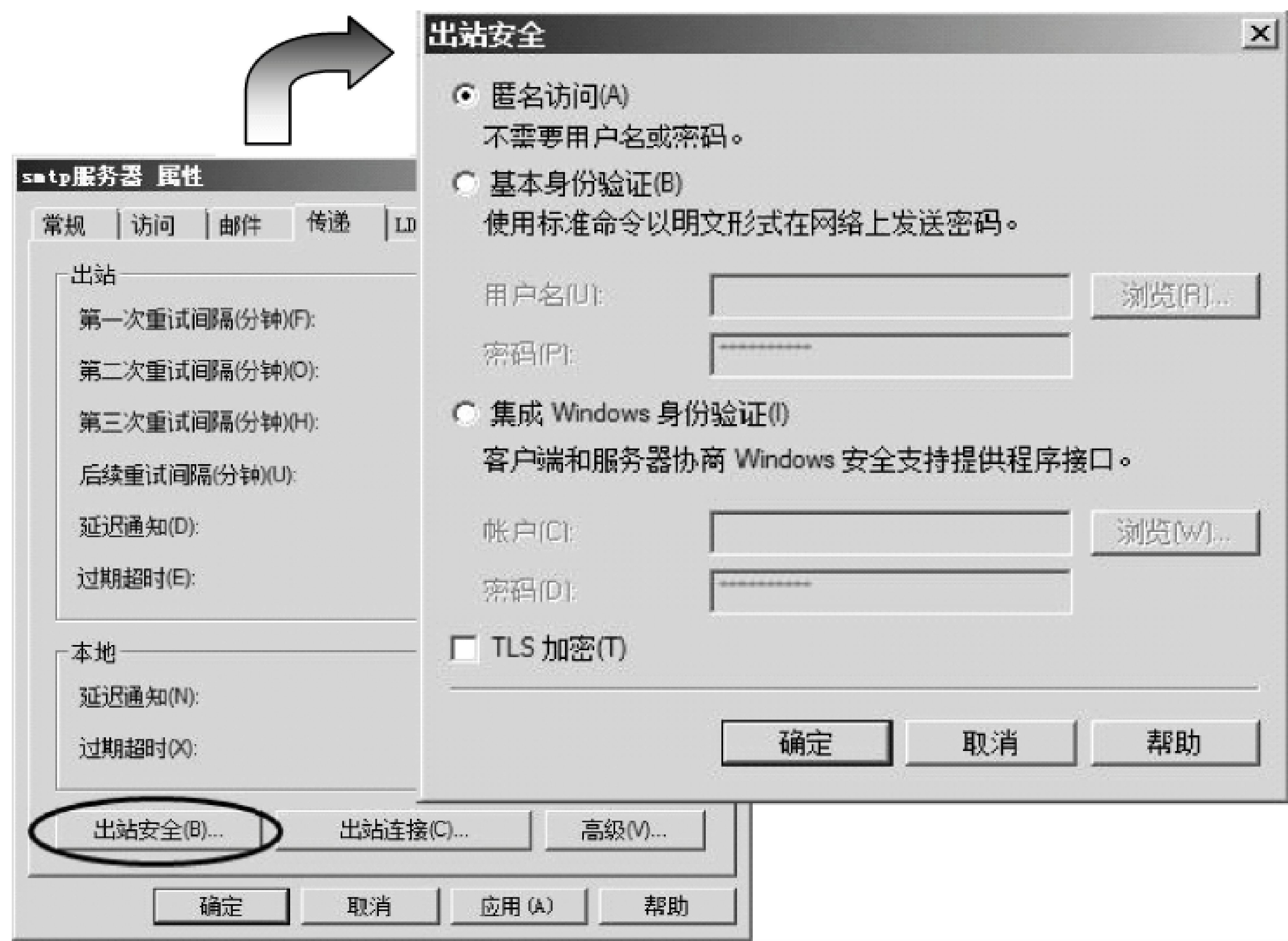



图 13-22　出站连接的身份验证设置

### 13.3.7 连接的 IP 地址限制

SMTP 服务器可以允许或拒绝某一个或某一群用户的连接,设置的方法是:右击 SMTP 虚拟服务器,选择“属性”弹出菜单项,在“属性”对话框中选择“访问”选项卡。单击“连接”按钮,如图 13-23 所示。

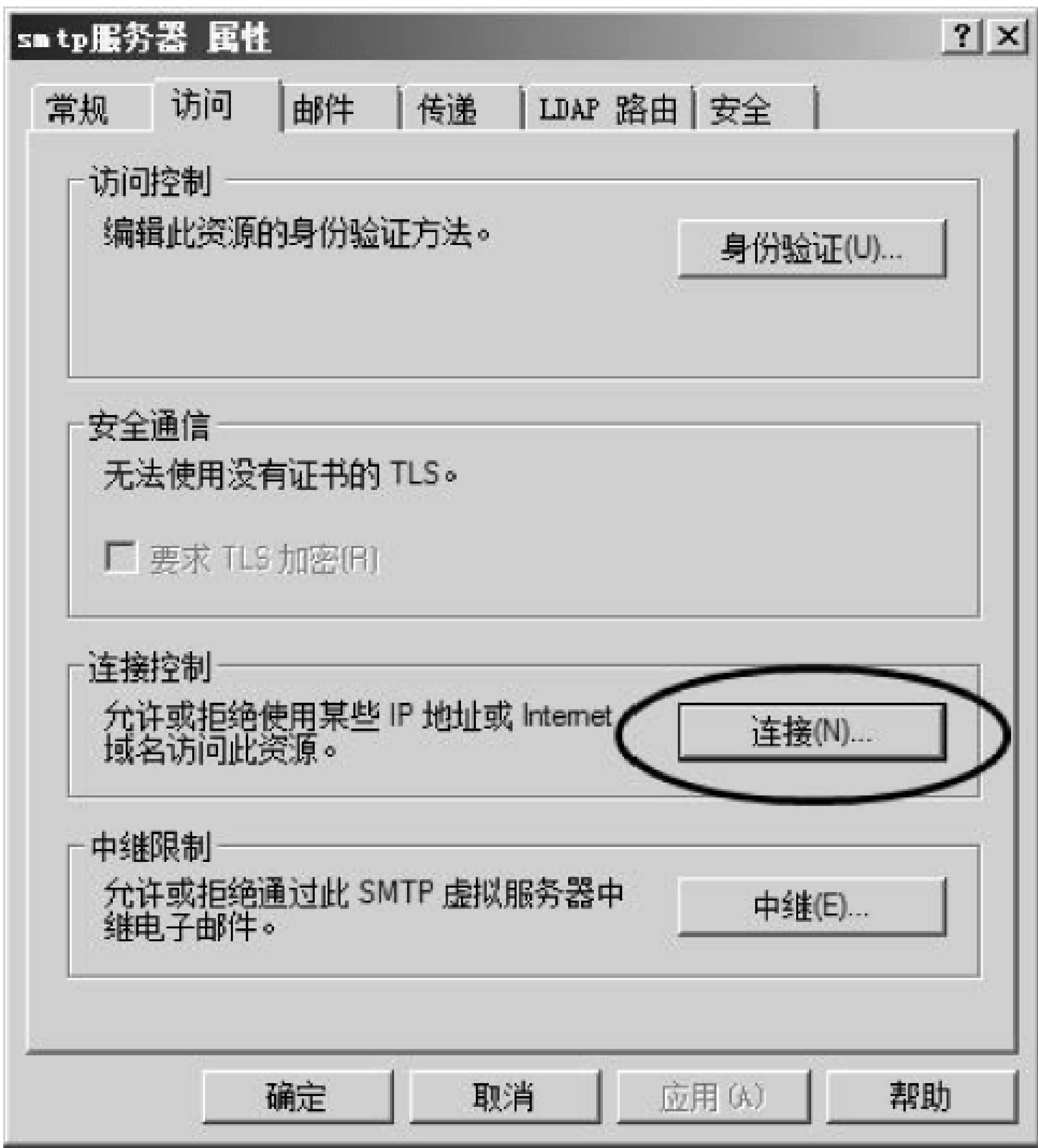



图 13-23 设置 SMTP 服务器的连接控制

在“连接”对话框中,选择“仅以下列表”为仅允许列表中的计算机访问 SMTP 服务器;选择“以下列表除外”为拒绝列表中的计算机访问 SMTP 服务器。单击“添加”按钮,打开“计算机”对话框,这里可以设置一台计算机或一个网段上的计算机,如图 13-24 所示。

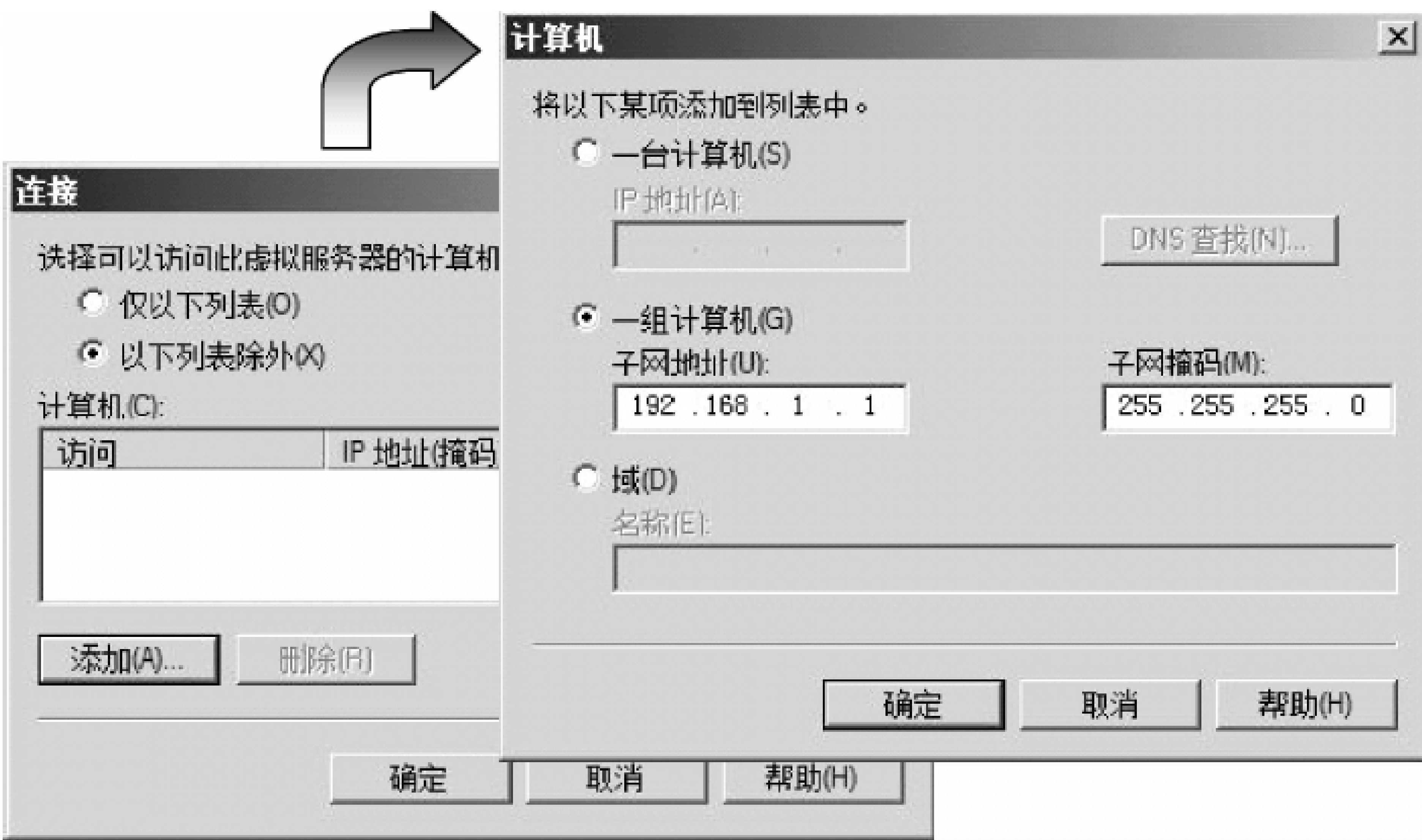



图 13-24 设置允许/拒绝访问的计算机

# 13.4　使用 SMTP 中继服务器转发邮件

为了模拟出 SMTP 中继服务器的中继效果，我们设计了如图 13-25 所示的网络结构。

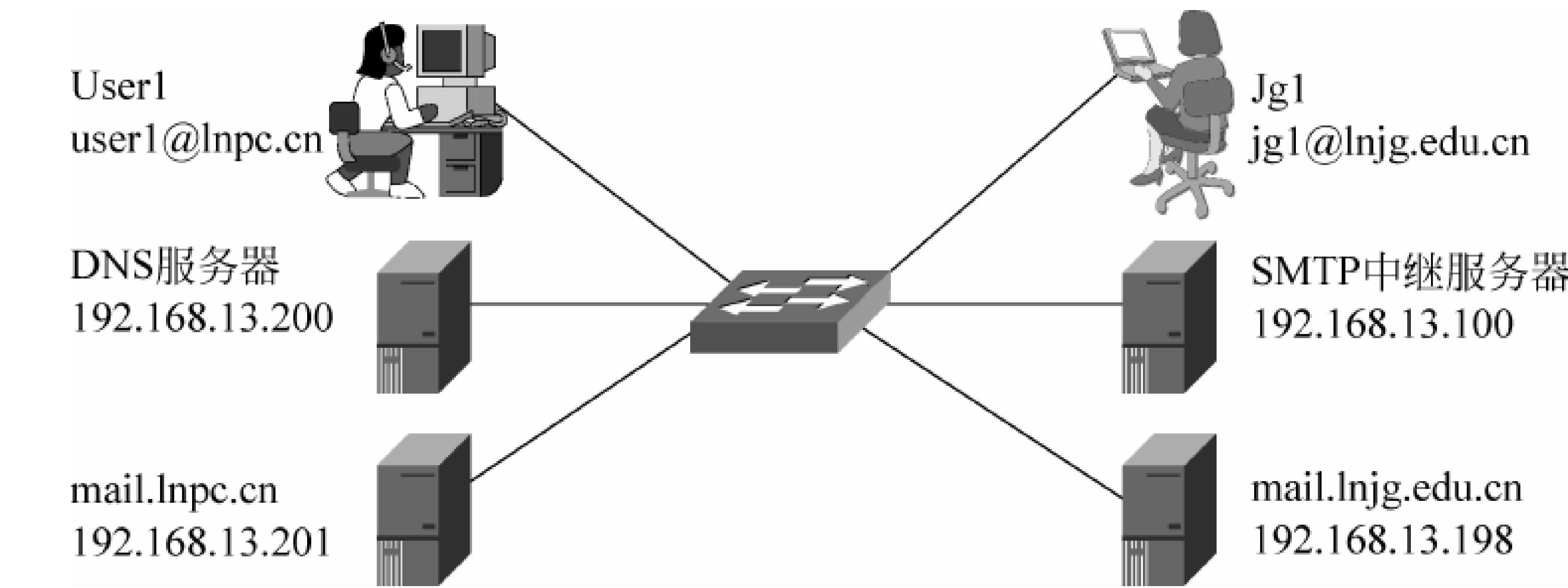



图 13-25　中继转发邮件的网络结构图

## 13.4.1　邮件服务器的设置

为了让邮件服务器把发出的邮件都传送到 SMTP 中继服务器，并且能接收 SMTP 中继服务器发出的邮件，需要对邮件服务器进行设置。

步骤 1：打开浏览器，输入 mail. lnpc. cn：8080，以管理员身份登录邮件服务器，点击窗口左侧的“系统设置”，打开如图 13-26 所示的界面。单击“SMTP 服务”。




图 13-26　邮件服务器系统设置界面

步骤 2：打开如图 13-27 所示界面，单击"中继网关列表"。

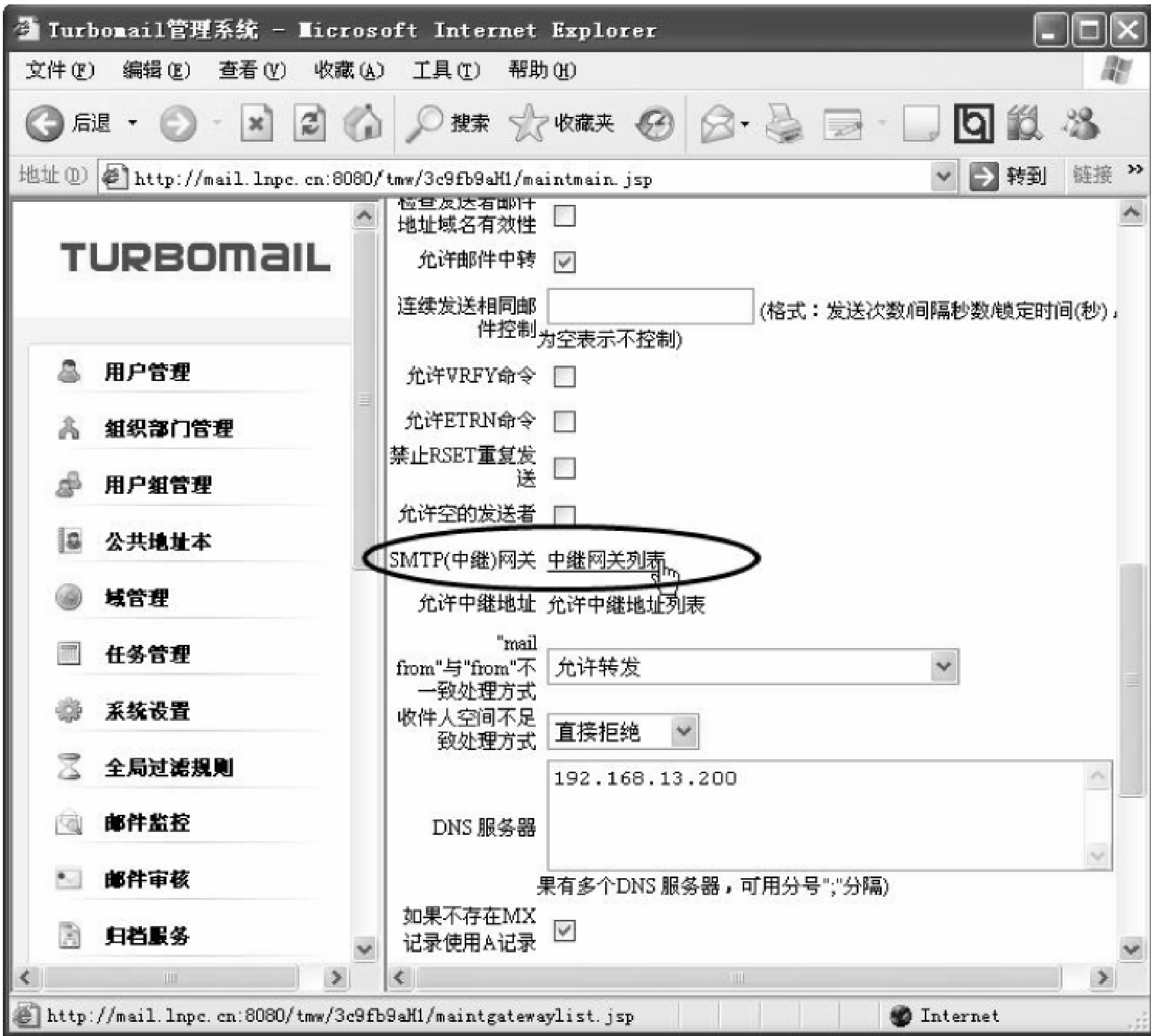



图 13-27　设置中继网关

步骤 3：单击图 13-28 所示的"增加"按钮。




图 13-28　增加中继网关

步骤 4：输入中继网关地址 192.168.13.100，并单击“保存”按钮，如图 13-29 所示。




图 13-29　输入中继网关地址

步骤 5：返回到 SMTP 设置页面，单击“允许中继地址列表”，如图 13-30 所示。




图 13-30　设置允许中继地址列表

步骤 6：输入“允许中继地址列表”192.168.13.100，如图 13-31 所示。




图 13-31 输入允许中继地址列表

同样的步骤，把邮件服务器 mail.lnjg.edu.cn 的中继服务器列表和允许中继地址列表也设置为 192.168.13.100。设置完成两个邮件服务器后，需要把两个邮件服务重新启动一下，设置才能发挥作用。

## 13.4.2 设置中继限制

SMTP 虚拟服务器默认情况下只接收传入邮件，不能外传邮件，也就是说，如果 SMTP 服务器接收到属于它管辖的域范围的邮件，则予以中继，如果 SMTP 服务器接收到不属于它的负责的域的邮件，则予以拒绝，不给以中继。比如 SMTP 服务器负责的域是 lnpc.cn，现在有一封邮件是发给 tom@lnpc.cn，则 SMTP 服务器会接收此邮件。若它收到了一封发给 bob@sina.com.cn 的邮件，则它不会接收，因为 sina.com.cn 不是它负责的域。

设置中继限制的步骤如下。

在 SMTP 服务器上，依次选择“开始”→“管理工具”→“Internet 信息服务(IIS)6.0 管理器”，在打开的“Internet 信息服务(IIS)6.0 管理器”窗口中右击“SMTP Virtual Server #1”，选择“属性”弹出菜单项，在“属性”对话框中选择“访问”选项卡。单击“中继”按钮，打开“中继限制”对话框。

- 仅以下列表：表示仅列表中的计算机被中继。
- 以下列表除外：表示列表中的计算机被拒绝，不予中继。

单击"添加"按钮,将添加被中继/被拒绝的计算机,如图 13-32 所示为允许 192.168.13.0 网段访问中继服务器。另外,若选择了"不管上表中如何设置,所有通过身份验证的计算机都可以进行中继",只要用户提供了有效的用户名和密码,SMTP 服务器就为它提供邮件中继服务。

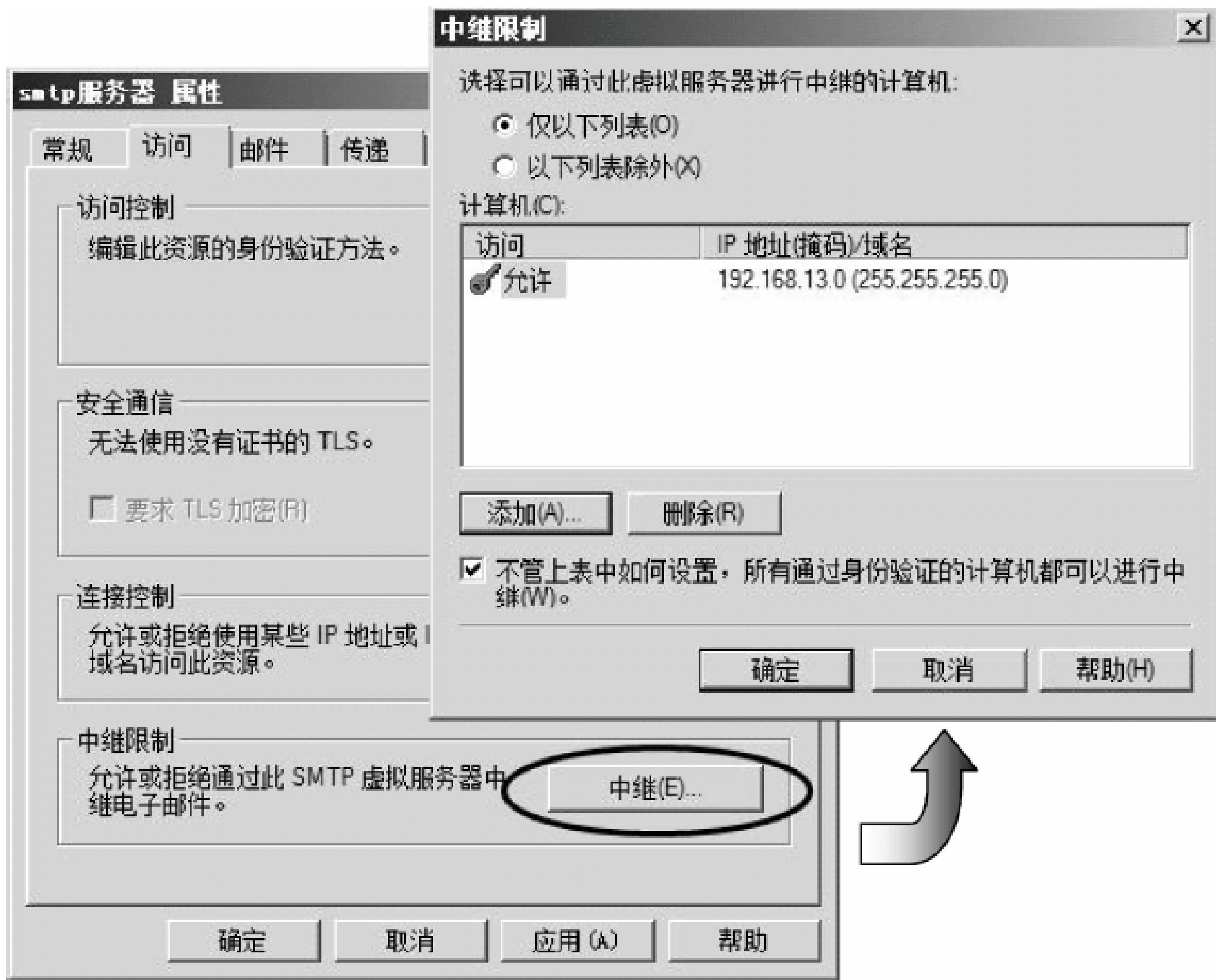



图 13-32　设置 SMTP 服务器的中继限制

### 13.4.3　通过中继发送邮件

通过 Web 方式或者邮件客户端用帐号 user1@lnpc.cn 登录 mail.lnpc.cn 邮件服务器,给 jg1@lnjg.edu.cn 发送邮件。用 jg1@lnjg.edu.cn 账号登录 mail.lnjg.edu.cn 服务器,接收电子邮件。

如果 jg1 没有收到电子邮件,请注意检查以下设置。

(1) 检查 SMTP 服务是否启动。

(2) 检查 SMTP 服务的中继限制是否允许邮件服务器把邮件发送到中继服务器。

(3) 检查邮件服务器的中继网关列表以及允许中继地址列表与中继服务器的地址是否相符合。

(4) 检查 DNS 服务器两个域下的 mail 域名 A 记录与 MX 记录设置的是否正确。

## 实验 18　邮件服务器的配置

### 1. 实验目标

(1) 通过安装配置邮件服务器,理解邮件发送的过程及相关协议。

(2) 通过安装配置 SMTP 中继服务器，实现邮件的中继传输，了解中继服务器的架设过程及其作用。

**2. 实验准备**

(1) 两台安装了 Windows Server 2008 的服务器：一台安装配置 DNS 服务器，另一台安装邮件服务器；一台安装了 Windows XP 或 Windows 7 的客户机。或者一台安装了虚拟机的性能较好的计算机，虚拟机中安装了 Windows Server 2008，在其上配置 DNS 和邮件服务器，客户机中安装 Windows XP 或 Windows 7。

(2) 四台安装了 Windows Server 2008 的服务器，其中两台将用于安装邮件服务器，一台用于安装 DNS 服务器，一台用于安装 SMTP 中继服务器。

(3) 交换机一台。

**3. 实验内容**

(1) 参照 13.2 节，安装并配置 DNS 服务器，添加域名 mail.abc.com 及 MX 记录，指向邮件服务器所在的服务器的 IP 地址；安装并配置邮件服务器，在其中创建 abc.com 域，创建两个账号 user1 和 user2，在客户机上通过 Web 方式或 Outlook Express 登录邮件服务器，实现两个账号之间互发 E-mail。

(2) 参照 13.3 小节，在服务器 1、2 上安装邮件服务器软件，其中一台创建域 abc.com，并创建账号 user1@abc.com；另一台创建 xyz.com，并创建 user2@xyz.com 账号。

在服务器 3 上安装配置 DNS 服务器，创建两个正向解析域 abc.com 和 xyz.com；在 abc.com 下创建 A 记录 mail.abc.com，MX 记录；在 xyz.com 下创建 A 记录 mail.xyz.com，MX 记录。

在服务器 4 上安装配置 SMTP 中继服务器，允许两个邮件服务器访问 SMTP 中继服务器。

在两个邮件服务器上配置中继网关地址及允许中继地址列表，指向 SMTP 服务器的 IP 地址。

在客户端上通过 Web 方式或 Outlook Express 登录邮件服务器，实现 user1@abc.com 与 user2@xyz.com 之间互发邮件。

# 思考与练习

**一、填空题**

1. SMTP 的全称是________，中文含义是________。

2. POP3 的英文全称是________，中文含义是________。

3. IMAP4 的英文全称是________，中文含义是________。

**二、选择题**

1. DNS 中邮件交换记录的标志是(　　)。

　A. A　　B. PTR　　C. CNAME　　D. MX

2. 电子邮件使用的主要协议有(　　)。
   A. SMTP　B. POP　C. MIME　D. 以上都是
3. 收发 E-mail 的常用客户端软件是(　　)。
   A. Outlook Express　B. CuteFTP
   C. Word　D. PowerPoint
4. E-mail 送信就是靠(　　)。
   A. FTP　B. POP3　C. HTTP　D. SMTP
5. E-mail 收信就是靠(　　)。
   A. SMTP　B. HTTP　C. POP3　D. FTP
6. E-mail 送信使用的端口号是(　　)。
   A. 25　B. 21　C. 80　D. 110
7. E-mail 收信使用的端口号是(　　)。
   A. 21　B. 110　C. 80　D. 25
8. E-mail 位址，b90123456@lnpc.cn，其中 b90123456 是(　　)。
   A. mail 主机名称　B. at
   C. 账号名称　D. 以上皆非

**三、问答题**

1. 如何通过电子邮件服务器传递邮件？
2. 为什么要架设 SMTP 中继服务器？
3. DNS 服务器中邮件交换记录 MX 起到什么作用？没有它可以吗？

# 参考文献


[1] 谢希仁. 计算机网络.第 5 版. 北京：电子工业出版社,2008.

[2] Richard Deal 著.张波,胡颖琼译. CCNA 学习指南.北京：人民邮电出版社,2009.

[3] 曹炯清. 网络互联技术与实训. 北京：科学出版社,2009.

[4] 石铁峰. 计算机网络技术. 北京：清华大学出版社,2010.

[5] 尚晓航. 计算机网络技术基础. 北京：高等教育出版社,2008.

[6] 杨云,马立新,金月光. Linux 网络操作系统与实训. 北京：中国铁道出版社,2008.

[7] 刘凯,李晶晶. Linux 服务器架设项目教程. 北京：电子工业出版社,2011.

[8] 卢豫开. Windows Server 2008 网络服务. 北京：机械工业出版社,2011.

[9] 宁蒙. Windows Server 2008 配置实训教程. 北京：机械工业出版社,2011.

[10] 王建平. 计算机组网技术——基于 Windows Server 2008. 北京：人民邮电出版社,2011.

[11] 丛书编委会. 交换机/路由器的配置与管理. 北京：中国电力出版社,2008.